

z/OS



Security Server RACF Messages and Codes

z/OS



Security Server RACF Messages and Codes

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 315.

Fourth Edition, September 2002

This is a major revision of SA22–7686–02. This edition applies to Version 1 Release 4 of z/OS (5694-A01), Version 1 Release 4 of z/OS.e (5655-G52), and to all subsequent releases and modifications until otherwise indicated in new editions.

Order documents through your IBM® representative or the IBM branch office serving your locality. Documents are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this document, or you may address your comments to the following address:

International Business Machines Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+845+432-9405

FAX (Other Countries):

Your International Access Code +1+845+432-9405

IBMLink™ (United States customers only): IBMUSM10(MHVRCFS)

Internet e-mail: mhvrcfs@us.ibm.com

World Wide Web: <http://www.ibm.com/servers/eserver/zseries/zos/webqs.html>

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this document
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1994, 2002. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	vii
Intended audience	vii
How to use this document	vii
Where to find more information	viii
Softcopy publications	viii
RACF courses	viii
Using LookAt to look up message explanations.	ix
Accessing z/OS licensed documents on the Internet	ix
IBM systems center publications	x
Other sources of information	x
IBM discussion areas	x
Internet sources	x
To request copies of IBM publications	xii

Summary of changes	xiii
---------------------------	------

Chapter 1. ICH Messages for the system operator.	1
Routing and descriptor codes	1
Descriptor code descriptions	1
Routing code descriptions	2
SAF initialization operator messages	2
RACROUTE REQUEST=VERIFY operator messages	4
RACF processing messages	5
RACF initialization messages	24
RACF Status Messages	41
RACROUTE REQUEST=AUTH Operator Messages.	42
RACROUTE REQUEST=DEFINE Operator Messages	43

Chapter 2. ICH messages for RACF commands	45
ADDGROUP command messages	47
ADDUSER command messages	49
CONNECT command messages	51
REMOVE command messages	53
DELUSER command messages	55
DELGROUP command messages	57
PERMIT command messages	58
PASSWORD command messages	61
ADDSD and DELDSD command messages	63
RDEFINE Command Messages	69
RALTER command messages	73
RDELETE command messages	77
RLIST command messages	79
SETROPTS command messages	80
RVARY command messages	91
ALTGROUP command messages	95
ALTUSER command messages	98
ALTDSD command messages	102
LISTUSER command messages	107
SEARCH command messages	108
LISTGRP command messages	111
LISTDSD command messages	112

Chapter 3. Miscellaneous RACF ICH messages	115
---	-----

RACF manager error messages.	115
RACF Report Writer (RACFRW) messages	117
Data Security Monitor (DSMON) messages	119
RACF miscellaneous messages.	124
Chapter 4. IRR RACF database initialization messages	127
Chapter 5. IRR messages for the system operator.	131
Routing and descriptor codes	131
Descriptor code descriptions	131
Routing code descriptions	132
VERIFY and VERIFYX messages	132
RACF processing messages	134
IRRDPI00 command messages	139
RACROUTE REQUEST=AUTH VLF messages	139
RACROUTE REQUEST=VERIFY NJE messages (Part 1)	140
RACF user ID and group ID mapping messages	142
Dynamic started task messages	142
RACROUTE REQUEST=VERIFY NJE messages (Part 2)	143
VLF cache messages	143
RACF/DB2 external security module messages	143
Chapter 6. IRR messages for commands, utilities, and other tasks	147
Messages common to several commands	148
Dynamic parse (IRRDPI00) messages	148
RACF cross-reference utility (IRRUT100) messages	168
RACF database verification (IRRUT200) messages	169
RACF Block Update Command (BLKUPD) messages.	176
RACF database split/merge utility (IRRUT400) messages	181
Internal reorganization of aliases utility (IRRIRA00) messages	186
RACF database unload utility (IRRDPU00) and RACF SMF data unload utility (IRRADU00) messages	190
RACF remove ID utility (IRRRID00) messages	200
REXX RACVAR messages	202
RACF subsystem messages	202
DISPLAY command messages	219
RACDCERT command messages	222
R_PKIServ callable service messages	230
SIGNOFF command messages	233
RRSF send request handling task messages	236
RRSF PARMLIB and initialization messages	237
SET command messages	239
RRSF handshaking messages	241
RRSF connection local transaction program messages	245
RACLINK command messages	246
RACROUTE REQUEST=LIST messages	247
CACHECLS profile messages	248
TARGET command messages	250
RRSF connection receive transaction program messages	260
RRSF connection send transaction program messages	262
RRSF (RACF remote sharing facility) general messages	262
RRSF connection task messages	266
RRSF output handling task messages	267
RACLINK command messages	274
RACLINK command or RRSF output handling task messages	276
File allocation messages	281
RRSF enveloping messages	282

RRSF operational modes and coupling facility messages	287
Chapter 7. IKJ messages	293
Chapter 8. RACF abend codes	295
Chapter 9. RACF return codes	307
RACF Manager Return Codes	307
RACF Utilities Return Codes	310
Appendix. Accessibility	313
Using assistive technologies	313
Keyboard navigation of the user interface	313
Notices	315
Programming interface information.	316
Trademarks	316
Index	319

About this document

This document supports z/OS (5694-A01) and z/OS.e (5655-G52) and contains information about the Resource Access Control Facility (RACF), which is part of the Security Server. The Security Server supports these components:

- Resource Access Control Facility (RACF)
- DCE Security Server
- z/OS Firewall Technologies
- Lightweight Directory Access Protocol (LDAP) Server, which includes client and server function
- Open Cryptographic Enhanced Plug-ins (OCEP)
- Security Server Network Authentication Service
- PKI Services

This document includes the messages, abend codes, RACF manager return codes, and RACF utility return codes produced by the Resource Access Control Facility (RACF) component.

If you need explanations of return codes from RACF macros, see *z/OS Security Server RACROUTE Macro Reference*.

For information about the other components of the Security Server, see the documentation related to those components.

Intended audience

This document is intended for anyone who uses Security Server RACF and wants to know what caused a message to be displayed and what corrective action, if any, needs to be taken.

How to use this document

The messages and codes in this document have been organized into chapters so that the documentation can be separated for easy use (if desired) according to the needs of the installation.

Messages are generally arranged in alphanumeric order by message identifier.

Most RACF messages have message identifiers. If you receive a message without a message identifier, your system may be suppressing the display of message numbers. Enter the following command and re-create the condition that caused the message to be displayed: `PROFILE WTPMSG MSGID`

If you have a message identifier, you might find the index helpful in finding the message itself.

In this document:

- Chapter 1, “ICH Messages for the system operator” on page 1 lists and explains the system operator messages that RACF routes to a system console or a security console.
- Chapter 2, “ICH messages for RACF commands” on page 45 lists and explains messages prefixed by ICH that are issued by RACF commands.
- Chapter 3, “Miscellaneous RACF ICH messages” on page 115 lists and explains miscellaneous messages prefixed by ICH.
- Chapter 4, “IRR RACF database initialization messages” on page 127 lists and explains messages prefixed by IRR that are issued during RACF database initialization.
- Chapter 5, “IRR messages for the system operator” on page 131 lists and explains messages prefixed by IRR that can go to the system operator.

- Chapter 6, “IRR messages for commands, utilities, and other tasks” on page 147 lists and explains messages prefixed by IRR that are issued by RACF commands, utilities, and other tasks.
- Chapter 7, “IKJ messages” on page 293
- Chapter 8, “RACF abend codes” on page 295 lists and explains the RACF-related abend codes that the system issues to indicate the abnormal completion of a task. Completion codes appear in hexadecimal.
- Chapter 9, “RACF return codes” on page 307 lists and explains the return codes from RACF manager and RACF utilities.
- An index is provided to help find messages.

Where to find more information

Where necessary, this document references information in other publications. For complete titles and order numbers for all elements of z/OS™, see *z/OS Information Roadmap*.

Softcopy publications

The RACF® library is available on the following CD-ROMs. The CD-ROM online library collections include Library Reader™, which is a program that enables you to view the softcopy documents.

SK3T-4269 *z/OS Version 1 Release 4 Collection*

This collection contains the set of unlicensed documents for the current release of z/OS in both BookManager® and Portable Document Format (PDF) files. You can view or print the PDF files with the Adobe Acrobat reader.

SK3T-4272 *z/OS Security Server RACF Collection*

This softcopy collection kit contains the Security Server library for z/OS in both BookManager and Portable Document Format (PDF) files. You can view or print the PDF files with the Adobe Acrobat reader.

SK2T-2180 *Online Library OS/390 Security Server RACF Information Package*

This softcopy collection contains the Security Server library for OS/390. It also contains the RACF/MVS Version 2 product libraries, the RACF/VM 1.10 product library, product documents from the OS/390® and VM collections, International Technical Support Organization (ITSO) documents (known as Redbooks™), and Washington System Center (WSC) documents (known as orange books) that contain information related to RACF. The collection does not contain any licensed publications. By using this CD-ROM, you have access to RACF-related information from IBM products such as OS/390, VM/ESA®, CICS®, and NetView®.

SK3T-7876 *IBM eServer zSeries™ Redbooks Collection*

This softcopy collection contains a set of documents called Redbooks that pertain to zSeries subject areas ranging from e-business application development and enablement to hardware, networking, Linux, solutions, security, Parallel Sysplex® and many others.

SK2T-2177 *IBM Redbooks S/390® Collection*

This softcopy collection contains a set of documents called Redbooks that pertain to S/390 subject areas ranging from application development and enablement to hardware, networking, security, Parallel Sysplex and many others.

RACF courses

The following RACF classroom courses are available:

ES840 *Implementing RACF Security for CICS/ESA® and CICS/TS*

H3917 *Basics of OS/390 Security Server RACF Administration*

H3927 *Effective RACF Administration*

ES88A *Exploiting the Features of OS/390 Security Server RACF*

IBM provides a variety of educational offerings for RACF. For more information about classroom courses and other offerings, do any of the following:

- See your IBM representative
- Call 1-800-IBM-TEACH (1-800-426-8322)

Using LookAt to look up message explanations

LookAt is an online facility that allows you to look up explanations for most messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can access LookAt from the Internet at:

<http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/>

or from anywhere in z/OS where you can access a TSO/E command line (for example, TSO/E prompt, ISPF, z/OS UNIX System Services running OMVS). You can also download code from the *z/OS Collection* (SK3T-4269) and the LookAt Web site that will allow you to access LookAt from a handheld computer (Palm Pilot VIIx suggested).

To use LookAt as a TSO/E command, you must have LookAt installed on your host system. You can obtain the LookAt code for TSO/E from a disk on your *z/OS Collection* (SK3T-4269) or from the **News** section on the LookAt Web site.

Some messages have information in more than one document. For those messages, LookAt displays a list of documents in which the message appears.

Accessing z/OS licensed documents on the Internet

z/OS licensed documentation is available on the Internet in PDF format at the IBM Resource Link™ Web site at:

<http://www.ibm.com/servers/resourceLink>

Licensed documents are available only to customers with a z/OS license. Access to these documents requires an IBM Resource Link user ID and password, and a key code. With your z/OS order you received a Memo to Licensees, (GI10-0671), that includes this key code.¹

To obtain your IBM Resource Link user ID and password, log on to:

<http://www.ibm.com/servers/resourceLink>

To register for access to the z/OS licensed documents:

1. Sign in to Resource Link using your Resource Link user ID and password.
2. Select **User Profiles** located on the left-hand navigation bar.

Note: You cannot access the z/OS licensed documents unless you have registered for access to them and received an e-mail confirmation informing you that your request has been processed.

Printed licensed documents are not available from IBM.

1. z/OS.e™ customers received a Memo to Licensees, (GI10-0684) that includes this key code.

You can use the PDF format on either **z/OS Licensed Product Library CD-ROM** or IBM Resource Link to print licensed documents.

IBM systems center publications

IBM systems centers produce documents known as red and orange books that can help you set up and use RACF. These documents have not been subjected to any formal review nor have they been checked for technical accuracy, but they represent current product understanding (at the time of their publication) and provide valuable information on a wide range of RACF topics. They are not shipped with RACF; you must order them separately. A selected list of these documents follows. Other documents are available, but they are not included in this list, either because the information they present has been incorporated into IBM product manuals or because their technical content is outdated.

G320-9279	<i>Systems Security Publications Bibliography</i>
GG22-9396	<i>Tutorial: Options for Tuning RACF</i>
GG24-3378	<i>DFSMS and RACF Usage Considerations</i>
GG24-3451	<i>Introduction to System and Network Security: Considerations, Options, and Techniques</i>
GG24-3524	<i>Network Security Involving the NetView Family of Products</i>
GG24-3970	<i>Elements of Security: RACF Overview - Student Notes</i>
GG24-3971	<i>Elements of Security: RACF Installation - Student Notes</i>
GG24-3972	<i>Elements of Security: RACF Advanced Topics - Student Notes</i>
GG24-3984	<i>RACF Macros and Exit Coding</i>
GG24-4282	<i>Secured Single Signon in a Client/Server Environment</i>
GG24-4453	<i>Enhanced Auditing Using the RACF SMF Data Unload Utility</i>
GG26-2005	<i>RACF Support for Open Systems Technical Presentation Guide</i>
GC28-1210	<i>System/390® MVS™ Sysplex Hardware and Software Migration</i>
SG24-4704	<i>OS/390 Security Services and RACF-DCE Interoperation</i>
SG24-4820	<i>OS/390 Security Server Audit Tool and Report Application</i>
SG24-5158	<i>Ready for e-business: OS/390 Security Server Enhancements</i>
SG24-5339	<i>The OS/390 Security Server Meets Tivoli®: Managing RACF with Tivoli Security Products</i>

Other sources of information

IBM provides customer-accessible discussion areas where RACF may be discussed by customer and IBM participants. Other information is also available through the Internet.

IBM discussion areas

- | IBM provides *ibm.servers.mvs.racf* newsgroup for discussion of RACF-related topics. You can find this
- | newsgroup on news (NNTP) server *news.software.ibm.com* using your favorite news reader client.

Internet sources

The following resources are available through the Internet to provide additional information about the RACF library and other security-related topics:

- **Online library**

To view and print online versions of the z/OS publications, use this address:

<http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>

- **Redbooks**

The documents known as Redbooks that are produced by the International Technical Support Organization (ITSO) are available at the following address:

<http://www.ibm.com/redbooks/>

- **Enterprise systems security**

For more information about security on the S/390 platform, OS/390, and z/OS, including the elements that comprise the Security Server, use this address:

<http://www.ibm.com/servers/eserver/zseries/zos/security/>

- **RACF home page**

You can visit the RACF home page on the World Wide Web using this address:

<http://www.ibm.com/servers/eserver/zseries/zos/racf/>

- **RACF-L discussion list**

Customers and IBM participants may also discuss RACF on the RACF-L discussion list. RACF-L is not operated or sponsored by IBM; it is run by the University of Georgia.

To subscribe to the RACF-L discussion and receive postings, send a note to:

listserv@listserv.uga.edu

Include the following line in the body of the note, substituting your first name and last name as indicated:

`subscribe racf-l first_name last_name`

To post a question or response to RACF-L, send a note, including an appropriate Subject: line, to:

racf-l@listserv.uga.edu

- **Sample code**

You can get sample code, internally-developed tools, and exits to help you use RACF. This code works in our environment, at the time we make it available, but is not officially supported. Each tool or sample has a README file that describes the tool or sample and any restrictions on its use.

To access this code from a Web browser, go to the RACF home page and select the “Downloads” topic from the navigation bar, or go to <ftp://ftp.software.ibm.com/eserver/zseries/zos/racf/>.

The code is also available from [ftp.software.ibm.com](ftp://ftp.software.ibm.com) through anonymous FTP. To get access:

1. Log in as user **anonymous**.
2. Change the directory, as follows, to find the subdirectories that contain the sample code or tool you want to download:

```
cd eserver/zseries/zos/racf/
```

An announcement will be posted on the RACF-L discussion list and on newsgroup *ibm.servers.mvs.racf* whenever something is added.

Note: Some Web browsers and some FTP clients (especially those using a graphical interface) might have problems using [ftp.software.ibm.com](ftp://ftp.software.ibm.com) because of inconsistencies in the way they implement the FTP protocols. If you have problems, you can try the following:

- Try to get access by using a Web browser and the links from the RACF home page.
- Use a different FTP client. If necessary, use a client that is based on command line interfaces instead of graphical interfaces.
- If your FTP client has configuration parameters for the type of remote system, configure it as UNIX[®] instead of MVS.

Restrictions

Because the sample code and tools are not officially supported,

- There are no guaranteed enhancements.
- No APARs can be accepted.

To request copies of IBM publications

Direct your request for copies of any IBM publication to your IBM representative or to the IBM branch office serving your locality.

There is also a toll-free customer support number (1-800-879-2755) available Monday through Friday from 6:30 a.m. through 5:00 p.m. Mountain Time. You can use this number to:

- Order or inquire about IBM publications
- Resolve any software manufacturing or delivery concerns
- Activate the program reorder form to provide faster and more convenient ordering of software updates

Summary of changes

Summary of changes for SA22-7686-03 z/OS Version 1 Release 4

This document contains information previously presented in z/OS SecureWay Security Server RACF Messages and Codes, SA22-7686-02, which supports z/OS Version 1 Release 3.

The following summarizes the changes to that information.

New information:

The following messages are added:

Information is added to indicate this document supports z/OS.e.

RACF Processing Messages: ICH426I, ICH427I, ICH428I, ICH429I, ICH430I

SETROPTS Command Messages: ICH14076I, ICH14077I (are issued instead of ICH14037 and ICH14038)

RACDCERT Command Messages: IRRD150I, IRRD151I, IRRD152I, IRRD153I, IRRD154I

RACF Initialization Messages: ICH578I, ICH580I

Dynamic Parse Messages: IRR52174I, IRR52175I, IRR52176I, IRR52177I, IRR52178I, IRR52179I, IRR52180I, IRR52181I, IRR52182I, IRR52183I, IRR52184I, IRR52185I, IRR52186I, IRR52187I

SEARCH Command Messages: ICH31028I

Changed information:

The following messages are changed:

RACDCERT Command Messages: IRRD135I

RACF Initialization Messages: ICH542I, ICH577E

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Starting with z/OS V1R2, you may notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

Summary of changes for SA22-7686-02 z/OS Version 1 Release 3

This document contains information previously presented in z/OS SecureWay Security Server RACF Messages and Codes, SA22-7686-01, which supports z/OS Version 1 Release 2.

The following summarizes the changes to that information.

New information:

An appendix with z/OS product accessibility information was added.

The following messages are added:

RACF Processing Messages: ICH408I

SAF Initialization Operator Messages: ICH010I, ICH011I, ICH012I

IRRDPI00 Command Messages: IRR545I, IRR546I

R_PKIServ Callable Services Messages: IRRD201I, IRRD202I, IRRD203I, IRRD204I, IRRD205I, IRRD206I, IRRD207I

Cache CLS Profile Messages: IRRL1000I, IRRL1001I, IRRL1002I, IRRL1003I

Dynamic Parse Messages: IRR52170I, IRR52171I, IRR52172I, IRR52173I

Changed information:

The following messages are changed:

RACF Processing Messages: ICH408I, IRR407I

RACF Initialization Messages: ICH577E

SAF Initialization Operator Messages: ICH001E

Dynamic Parse Messages: IRR52104I, IRR52142I

Deleted information:

The following messages are deleted:

- TSO command messages can now be found in the z/OS TSO/E Messages document. The following messages have been deleted from this document:
 - IKJ56701I
 - IKJ56702A
 - IKJ56702I
 - IKJ56718A

Note that the glossary has been removed from this document. You can now find the glossary in the *z/OS Security Server RACF Security Administrator's Guide*

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Summary of changes for SA22-7686-01 z/OS Version 1 Release 2

This document contains information previously presented in SA22-7686-00, which supports z/OS Version 1 Release 1.

The following summarizes the changes to that information.

New information

The following messages are added:

DELGROUP Command Messages: ICH05008I

RACF/DB2 External Security Module Messages: IRR912I, IRR913I

Changed information

The following messages are changed:

RACF Processing Messages: ICH408I

RACF Initialization Messages: ICH577E

RACF/DB2 External Security Module Messages: IRR900A, IRR901A, IRR902A, IRR903A, IRR909I

RACF DISPLAY Command Messages: IRRD103I, IRRD104I

RACF Remove ID Utility Messages: IRR68017I

This document contains terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability.

Chapter 1. ICH Messages for the system operator

This chapter lists the system operator messages that the Resource Access Control Facility (RACF) routes to a system console or a security console.

The format of these messages is:

ICHxnnnt text

where:

ICH identifies the message as a RACF message.

x identifies the RACF function, where:

- 0** = SAF initialization
- 3** = RACROUTE REQUEST=VERIFY macro
- 4** = RACF processing
- 5** = RACF initialization
- 7** = RACF status
- 8** = RACROUTE REQUEST=AUTH macro
- 9** = RACROUTE REQUEST=DEFINE macro

nn is the message serial number.

t is the type code, where:

- A** = Action; operator must perform a specific action.
- D** = Decision; operator must choose an alternative.
- E** = Eventual action required.
- I** = Information; no operator action is required.
- W** = Wait; processing stops until action is determined and performed.

text is the text of the message.

Routing and descriptor codes

The routing and descriptor codes for these messages are shown with the message explanations.

Descriptor code descriptions

Descriptor codes indicate the significance of a message. Specifically, descriptor codes let the user know the status of the system itself or that of a specific task:

- Has it stopped processing?
- Is it waiting for another action to be completed?
- Or, is it continuing to process?

In addition, this code determines how the system will display and delete the message.

Code Description

1 System Failure

The message indicates a catastrophic error. To continue, the operator must re-IPL the system or restart a major subsystem.

ICH001E • ICH002I

2 Immediate Action Required

The message indicates that the operator must perform an action immediately. The message issuer could be in a wait state until the action is performed, or the system needs the action as soon as possible to improve performance. The task waits for the operator to complete the action.

Note: When an authorized program issues a message with descriptor code 2, a DOM macro instruction *must* be issued to delete the message after the requested action is performed.

4 System Status

The message indicates the status of a system task or of a hardware unit.

6 Job Status

The message indicates the status of a job or job step.

Routing code descriptions

Routing codes send system messages to the consoles where they are to be displayed. To send a message to more than one console, RACF assigns more than one routing code to the message. For more information on message routing, see your MVS routing and descriptor codes documentation.

Code Description

1 Master Console Action

The message indicates a change in the status of the system. It demands action by the master console operator.

2 Master Console Information

The message indicates a change in the status of the system. It does not demand action; rather, it alerts the master console operator to a condition that may require action.

This routing code is used for any message that indicates job status when the status is not requested specifically by an operator inquiry. It is also used for processor and problem program messages to the system operator.

9 System Security

The message gives information about security checking, for example, a request for a password.

11 Programmer Information

The message is intended for the problem programmer. This routing code is used only when the program issuing the message cannot route the message to the programmer via the system output (SYSOUT) data set. The message appears in the job log.

Note: Routing code 11 is ignored if specified for a multiple-line WTO macro instruction.

SAF initialization operator messages

ICH001E SAF IS NOT ACTIVE, SDUMP TAKEN

Explanation: The system authorization facility (SAF) is not active. This message is preceded by another message which explains why and is followed by message ICH006D.

System Action: The SAF error exit requests a dump and issues message ICH006D.

ICH002I UNABLE TO OBTAIN STORAGE FOR SAF INITIALIZATION

Explanation: The system authorization facility (SAF) issued a GETMAIN macro for storage in the system queue area (SQA), which is subpool 265, to build the ICHSAFV control block. The GETMAIN failed.

System Action: The SAF error exit issues message ICH001E.

**ICH003I UNABLE TO LOCATE SAF ROUTER
(ICHSFR00) IN LPA**

Explanation: The system cannot locate the system authorization facility (SAF) load module, ICHSFR00, in the link pack area (LPA).

System Action: The SAF error exit issues message ICH001E.

**ICH004I SYSTEM ERROR DURING SAF
INITIALIZATION**

Explanation: During initialization of the system authorization facility (SAF), a program check occurred. The SAF error exit was invoked.

System Action: The SAF error exit issues message ICH001E.

ICH005I ACTIVE SAF EXIT: ICHRTX00

Explanation: The system authorization facility (SAF) installation exit, module ICHRTX00, is in use.

System Action: System initialization proceeds.

**ICH006D RE-IPL OR REPLY U TO CONTINUE
WITHOUT SAF**

Explanation: The system authorization facility (SAF) error exit issues this message after ICH001E to let the operator decide whether to continue without SAF or to re-IPL.

System Action: System initialization stops until the operator replies.

Operator Response: Reply U to continue initialization without SAF. Otherwise, correct the problem and re-IPL the system, so that SAF can be included.

**ICH007E ICHSFI00 NOT FOUND. REPLY 'U' TO
CONTINUE**

Explanation: During RACF initialization, the system cannot find the system authorization facility (SAF) initialization module, ICHSFI00, in SYS1.LINKLIB.

System Action: System initialization stops until the operator replies.

Operator Response: Reply U to continue initialization without SAF. Otherwise, correct the problem and re-IPL the system, so that SAF can be included.

ICH010I ACTIVE SAF EXIT: IRRSZT00

Explanation: The system authorization facility (SAF) installation exit module, IRRSZT00, has been loaded and is now in use.

System Action: System initialization proceeds.

**ICH011I UNABLE TO LOCATE SAF ROUTER
IRRSZR10 IN LPA**

Explanation: The system cannot locate the system authorization facility (SAF) load module, IRRSZR10, in the link pack area (LPA).

System Action: The SAF error exit issues message ICH001E.

**ICH012I FAILURE WHILE INITIALIZING POLICY
DIRECTOR SERVICES**

Explanation: An error occurred during the initialization of IBM Policy Director Authorization Services for z/OS and OS/390 support for SAF callable services.

System Action: A dump was requested. Processing continues, but IBM Policy Director Authorization Services for z/OS and OS/390 will not be able to provide support for SAF callable services, such as aznCreds (IRRSZC00) or aznAccess (IRRSZA00), and invocation of these services will fail. System initialization proceeds.

RACROUTE REQUEST=VERIFY operator messages

ICH301I **MAXIMUM PASSWORD ATTEMPTS BY SPECIAL USER** *userid* [AT TERMINAL *terminalid*.]

Explanation: The user specified by *userid* has made more than the permissible number of attempts to enter a password. If this was not a batch job, the last attempt was from the terminal specified by *terminalid*. Because the specified user has the SPECIAL attribute, the RACF security administrator has the option of not revoking the user. This message is followed by message ICH302D.

The permissible number of password attempts is set using the command

SETRPTS PASSWORD(REVOKE(*number_invalid_passwords*))

Destination: Descriptor code is 4. Routing code is 9.

has the option of not revoking the user. This message is followed by ICH304D.

Destination: Descriptor code is 4. Routing code is 9.

ICH302D **REPLY Y TO ALLOW ANOTHER ATTEMPT OR N TO REVOKE USERID** *userid*.

Explanation: This message, which is preceded by a number, follows message ICH301I.

System Action: If the response is Y, the specified user is allowed another attempt to log on. A failure during this attempt causes messages ICH301I and ICH302D to be reissued. If the response is N, the specified user ID is revoked.

Note: If there is no response to this message within 10 minutes, it will time out and be purged. If a reply is now issued for this message, the reply will be accepted, but you will receive the following message:

RPIMGR012E IUCV ERROR WITH CP: REPLY
CC=1, RC=9

Operator Response: Reply with either Y or N.

Destination: Descriptor code is 2. Routing code is 9.

Note: In multiple-user address spaces that have a single signon task (such as CICS or IMS), when the signon task issues the message, no other signons can occur until the operator has replied to the message.

ICH303I **INACTIVE INTERVAL EXCEEDED BY USER** *userid* (AT TERMINAL *terminalid*).

Explanation: The user specified by *userid* has not accessed the system and had the last access interval updated within the limit specified by SETROPTS INACTIVE(*unused-userid-interval*). If this was not a batch job, the last attempt was from the terminal specified by *terminalid*. Because the specified user has the SPECIAL attribute, the RACF security administrator

ICH304D **REPLY Y TO ACTIVATE USER OR N TO REVOKE USERID** *userid*.

Explanation: This message, which is preceded by a number, follows message ICH303I.

System Action: If the response is Y, the logon attempt by the specified user is allowed to continue. If the response is N, the specified user ID is revoked.

Operator Response: Reply with either Y or N.

Destination: Descriptor code is 2. Routing code is 9.

RACF processing messages

Note on the ICH408I messages

Message ICH408I is a set of messages that are displayed in multiple lines.

The first line of an ICH408I message identifies a user or job that had an authorization problem. The other lines of the messages (shown in this document following the explanation of **USER or JOB**) describe the request the user or job was issuing and the reason for the failure.

See the following example:

```
ICH408I USER(SMITH ) GROUP(DEPT60 ) NAME(R.L.SMITH )
ICH408I DEPT58.CLIST.CNTL CL(DATASET ) VOL(TSO035)
ICH408I INSUFFICIENT ACCESS AUTHORITY
ICH408I FROM DEPT58.CLIST.* (G)
ICH408I ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )
```

This message can be interpreted as:

User SMITH, a member of group DEPT60, whose name is R.L.SMITH, had INSUFFICIENT ACCESS AUTHORITY to resource DEPT58.CLIST.CNTL, which is in class DATASET and resides on volume TSO035.

The RACF profile protecting the resource is DEPT58.CLIST.*, and it is a generic profile.

The access attempted by SMITH was READ, and the access allowed by RACF was NONE.

Each set of ICH408I messages contains at least one line that describes the reason for failure, usually in the 2nd or 3rd line. Each line of reason for failure is listed and described in alphabetical order in this RACF Processing Messages section.

ICH408I **USER** (*userid*) **GROUP** (*group-name*)
NAME (*user-name*) **--or--** **JOB** (*jobname*)
STEP (*stepname*) [**SUBMITTER** (*userid*)]
[*resource-name*] [**CL**(*class-name*)] **--or--**
[**VOL**(*volume-id*)] [**FID**(*file-identifier*)]
[**ID**(*IPC-identifier*)] **--or--** [**FROM**
generic-profile-name (**G**)] [**ACCESS**
INTENT(*intent*) **ACCESS**
ALLOWED(*allowed*)] [**EFFECTIVE UID**
(*nnnnnnnnnn*)] [**EFFECTIVE GID**
(*nnnnnnnnnn*)]

Explanation: This message is issued when RACF detects an unauthorized request (a violation) made by a user or job. The user and group indicated in the first line of the ICH408I message are the execution user ID and group ID under which the job was to run.

If the message indicates a job and step instead of a user, group, and name, RACF could not find a valid ACEE containing user, group, and name information. This could occur for a started task that is not defined in the RACF started procedures table (ICHRIN03), if an entry in the started procedures table has an incorrect RACF group specified, or if the user's ACEE has been corrupted. If the submitting user ID is not the same as the execution user ID, the message includes an

additional line containing the submitting user ID, group, and node.

When the message is reporting an access failure for an z/OS UNIX file, the *resource name* is the pathname that was specified to the kernel syscall. It will not exist for the syscalls performed against open files (those in the "fxxxxx" format such as fchown). The FID (*file identifier*) is a unique 32-hex-digit identifier of the file. It is provided because multiple pathnames can be used to access the same file. This identifier will allow matching of accesses to the same file by different names.

When the message is reporting an access failure for an z/OS UNIX IPC key, the *resource name* is the IPC key name that was specified to the kernel syscall. It is displayed as a unique 8-hex-digit identifier. The ID (*IPC identifier*) is a unique decimal identifier of the resource. It is provided as additional information, that may be useful during auditing, although it is dynamically allocated by the kernel. It is a numeric value between 0 and 4294967295.

The meaning of the volume serial number shown in the VOL field varies. For a non-VSAM data set, it means the volume on which the data set resides. For a VSAM data set, it means the volume on which the catalog

ICH408I

containing the data set entry resides.

The phrase FROM *generic-profile-name* (G), if included in the message, identifies the generic profile that RACF used to check for access to the resource.

For further explanations of this message, check the message line that indicates what request was made. This is usually line 2 or 3. For example, it could be INSUFFICIENT ACCESS AUTHORITY. Find this message line among the explanations that follow for message ICH408I (arranged alphabetically), and read the explanation for that message line.

For attempts to use protected resources, the message shows the access attempted (ACCESS INTENT phrase) and the access permitted by RACF (ACCESS ALLOWED phrase). When the message is reporting an attempt to access an z/OS UNIX file or IPC key, the ACCESS INTENT (*intent*) is specified as "RWX", representing read, write or search/execute permission requested. More than one permission can be requested at a time. If a permission is not requested, the letter is replaced by a dash "-". ACCESS ALLOWED (*allowed*) is specified as "{OWNER/GROUP/OTHER/ACL USER/ACL GROUP/NO/RESTRICTED} RWX", where OWNER indicates the owner permission bits were used, GROUP indicates the group permission bits were used, OTHER indicates the other permission bits were used, ACL USER indicates that a specific user Access Control List (ACL) entry was used, ACL GROUP indicates a specific group ACL entry (or entries) was used, NO indicates that no permission bits were used, RESTRICTED indicates the OTHER bits were not used for a RESTRICTED user, and "RWX" represents the settings of the permission bits that were checked. ACCESS ALLOWED (NO --X) occurs if a superuser attempts to execute a file that does not have OWNER, GROUP, ACL, or OTHER execute permission. ACCESS ALLOWED (RESTRICTED —) occurs if a RESTRICTED user could have only gained file access via the OTHER bits, but the RESTRICTED.FILESYS.ACCESS profile in the UNIXPRIV class has forbidden this.

Note that while checking for group access, the group permission bits are treated as simply another GID ACL entry, if the process GID, or one of its supplemental GIDs matches the file owner GID. Several group entries may actually be checked, and access will be granted if any of them specifies the requested permissions. However, if none of the entries grants the requested access, there is no single entry that defines the access allowed. By convention, the permissions associated with the first relevant group entry encountered are what will be displayed in the message. See the z/OS UNIX information in the *z/OS Security Server RACF Security Administrator's Guide* for a description of the algorithm used to determine access when an ACL exists for a file or directory.

For violations occurring in the UNIX System Services environment, the user's effective UID and effective GID

are displayed in the message. These ids were used to determine the user's privilege for the intended operation. Note that they may not always match the ids defined in the relevant RACF USER and GROUP profiles, since UNIX System Services provides methods by which another identity can be assumed.

System Action: If the phrase RESOURCE NOT PROTECTED appears in the message with a warning, RACF allows the request to continue. If the phrase RESOURCE NOT PROTECTED appears in the message without a warning, RACF fails the request.

Notes:

1. When a user is denied access to a RACF-protected resource because of the return code from a RACROUTE REQUEST=AUTH installation exit routine, the user's allowed access may be inconsistent with the requested access. (For example, access allowed was ALTER, access requested was READ, but the request for access was denied.)
2. Authority checking for users with the restricted attribute bypasses checking of some authority granting mechanisms, such as the UACC. If a LISTUSER for the user ID shows that the user is restricted, the user's user ID or group name must be on the access list to allow access to the resource. See *z/OS Security Server RACF Security Administrator's Guide* for additional information on restricted access user IDs.
3. A user who has ALTER access authority to a DASD volume can scratch a data set on that volume even if the user does not have the required ALTER access authority to that particular data set. In this case, on systems without always-call, message ICH408I is issued even though the data set is scratched; on systems with always-call, the message is not issued.
4. The phrase "LOGON/JOB INITIATION/initACEE" may appear during logon processing; however, the logon may be successful. When RACF is active, logon verification can produce an error during RACF processing; however, the logon can proceed using an alternate method (for example, UADS). This error occurs if the installation does not use the RACF database to store security-related information for a particular user, but it does use an alternate method (such as UADS) for the logon application (for example, TSO) to perform user verification.
5. If the failure occurred for a z/OS UNIX System Services system function, RACF returns an error return code to the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See *z/OS UNIX System Services Programming: Assembler Callable Services Reference* to determine the action of the syscall functions.
6. If you see JOB/STEP, it indicates a default security environment for an undefined user. This can happen

if a started procedure is not defined correctly in the STARTED class or in ICHRIN03.

- If you used the STARTED class, make sure it was properly RACLIST REFRESHed after you added the profiles.
- If you used ICHRIN03, be sure to IPL the system with CLPA.

User Response: Follow the security procedures established for your installation. If no such procedures have been established, report the complete text of this message to the RACF security administrator.

Operator Response: Follow the security procedures established for your installation. If no such procedures have been established, report the complete text of this message to the RACF security administrator.

Problem Determination: Detailed information about the violation is available in the SMF type 80 record that RACF produces at the same time as this message. See *z/OS Security Server RACF Auditor's Guide* for information about reporting on the contents of the RACF SMF records.

Notes:

1. When RACF verifies a password during logon or when a batch job begins, the message includes NAME (???).
2. For users not defined to RACF, the job and step are indicated by *jobname* and *stepname*. For batch users, *stepname* is blank.

Destination: Descriptor code is 4. Routing codes are 9 and 11. This message is routed to the security console. All violations (except LOGON/JOB initiation/initACEE messages, command violations, and z/OS UNIX System Services violations) are issued as write-to-programmer (WTP) messages.

Note: A TSO/E user who is using z/OS UNIX System Services does not see the ICH408I messages.

ICH408I DEFINE - GROUP NOT DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource; for example, by way of RDEFINE for a general resource or ADDSD for a data set.

System Action: RACF prevents the request from completing.

User Response: Correct any spelling errors in the group ID and try again. If you cannot remember the correct group ID, ask your RACF security administrator to provide you with a valid group ID.

ICH408I DEFINE - INSUFFICIENT AUTHORITY

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource; for example, by way of RDEFINE for a general resource or ADDSD for a data set. This message can also be issued for certain types of create and rename requests.

System Action: RACF prevents the request from completing.

ICH408I DEFINE - RESOURCE ALREADY DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource; for example, by way of RDEFINE for a general resource or ADDSD for a data set.

System Action: RACF prevents the request from completing.

ICH408I DEFINE - RESOURCE NOT PROTECTED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a resource that requires RACF protection, such as an MVS data set when the SETROPTS PROTECTALL option is in effect.

System Action: RACF prevents the request from completing.

ICH408I DEFINE - USER IN SECOND QUALIFIER IS NOT RACF-DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource. The user specified a profile name in which the second qualifier was not a RACF-defined user ID.

System Action: RACF prevents the request from completing.

User Response: Correct the second qualifier in the profile name and try again.

ICH408I DEFINE - USER NOT MEMBER OF GROUP

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource.

System Action: RACF prevents the request from completing.

User Response: Correct any spelling errors in the group ID and try again. If you cannot remember the correct group ID, ask your RACF security administrator to provide you with a valid group ID.

ICH408I

ICH408I DEFINE - USER NOT RACF-DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource.

System Action: RACF prevents the request from completing.

ICH408I DEFINE - WARNING: INSUFFICIENT SECURITY LABEL AUTHORITY

Explanation: This error occurs when RACF detects an unauthorized attempt to define a resource that has a security label associated with it.

System Action: RACF allows the request to complete.

User Response: If the security label is misspelled, try again. You might need to log off and log on again with a different security label. For a list of security labels you can specify, enter the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

ICH408I DEFINE - WARNING: RESOURCE NOT PROTECTED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource.

System Action: RACF allows the request to complete.

ICH408I DEFINE - WARNING: SECURITY LABEL MISSING FROM USER, JOB, OR PROFILE

Explanation: RACF issues this message when a security label is missing from one of the following:

- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

and the SETROPTS MLACTIVE(WARNING) option is in effect.

System Action: RACF allows the request to complete.

User Response: If a line of this message indicates a profile in a RACF class, such as SMITH.CLIST CL(DATASET) VOL(D58000), the indicated resource profile is missing a security label. If a security label is not specified for the profile before the installation puts the SETROPTS MLACTIVE(FAILURES) option into effect, you will not be able to log on or submit the job.

ICH408I DELETE - INVALID VOLUME

Explanation: This error occurs when RACF detects an unauthorized attempt to delete a RACF-protected resource.

System Action: RACF prevents the request from completing.

ICH408I DELETE - RESOURCE NOT FOUND

Explanation: This error occurs when RACF detects an unauthorized attempt to delete a RACF-protected resource.

System Action: RACF prevents the request from completing.

ICH408I DIGITAL CERTIFICATE SUPPLIED TO AUTHENTICATE USER *userid* IS NOT TRUSTED. CERTIFICATE SERIAL NUMBER(*serial-number*) SUBJECT(*subject-name*) ISSUER(*issuer-name*).

Explanation: A user attempted to access a server using a digital certificate that is not trusted.

System Action: InitACEE processing ends.

User Response: Ensure the user is supplying the correct certificate. If the user is supplying the correct certificate, and it should be trusted, reissue the RACDCERT command with TRUST specified to change the status of the certificate, or certificate mapping.

ICH408I DIGITAL CERTIFICATE IS NOT DEFINED. CERTIFICATE SERIAL NUMBER (*serial-number*) SUBJECT(*subject-name*) ISSUER(*issuer-name*).

Explanation: A user attempted to access a server using a digital certificate that is not defined to RACF. RACF cannot determine a user ID for this user.

System Action: InitACEE processing ends.

User Response: Ensure the user is supplying the correct certificate. If the user is supplying the correct certificate, and it should be associated with a RACF user ID, use the RACDCERT command to ADD the certificate for the user, or associate it with a user ID with the MAP function. If a certificate mapping already exists for the certificate and it has additional criteria specified, check for an entry in SYS1.LOGREC to determine if an error was encountered attempting to locate the corresponding DIGTCRIT profile.

ICH408I FULL VIOLATION ON COMMAND
command

Explanation: This error occurs when RACF detects an unauthorized attempt to use a RACF command that would modify profiles on the RACF database.

System Action: RACF prevents the command from completing.

ICH408I INSUFFICIENT ACCESS AUTHORITY

Explanation: This error occurs when RACF detects an unauthorized attempt to access a RACF-protected resource.

System Action: RACF denies the requested access.

**ICH408I INSUFFICIENT AUTHORITY TO
EXTEND TO A NEW VOLUME**

Explanation: This error occurs when RACF detects an attempt to specify an unauthorized volume on the ADDVOL or CHGVOL operand.

System Action: RACF denies the request.

ICH408I INSUFFICIENT AUTHORITY TO
syscall-name [CMD(subcommand)]
[UNABLE TO PROCESS ACL]

Explanation: This error occurs when RACF detects an attempt to specify an z/OS UNIX function for which the user does not have authority. *Syscall-name* identifies the z/OS UNIX callable service that invoked RACF. *Subcommand* identifies the subcommand of *syscall-name*, where appropriate. If present, *subcommand* is either IPC_RMID or IPC_SET. The text ":UNABLE TO PROCESS ACL" will be displayed if a file access check detected that an ACL exists for the file, but it could not be retrieved. In this case, the "ACCESS INTENT ...ACCESS ALLOWED..." portion of ICH408I will not be displayed. This most likely indicates that a release level mismatch exists among nodes in a SYSPLEX. For example, if an ACL had been created for a file by an uplevel node, access attempts to this file from a downlevel node will fail with this message text. Similarly, if an ACL had been created for a file by an uplevel node, and the file system in which it resides has been subsequently mounted by a downlevel node, access attempts to this file will fail with this message text.

System Action: RACF returns an error return code to the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See *z/OS UNIX System Services Programming: Assembler Callable Services Reference* to determine the action of the syscall functions.

Programmer Response: Provide appropriate information about the failure to the user of your program, based on the function invoked and the return

codes received. If "UNABLE TO PROCESS ACL" is displayed, then you must upgrade all nodes in the sysplex to a level of code which supports ACLs. If you require immediate access to the file, try unmounting the file system from the current node, remounting it on an uplevel node, and accessing it from an uplevel node.

**ICH408I INSUFFICIENT SECURITY LABEL
AUTHORITY**

Explanation: This error occurs when RACF detects one of the following:

- An attempt to access a resource that has a security label associated with it, and the access cannot be authorized because the requester is running under an inappropriate security label
- An attempt to access a resource that has no security label associated with it and the access cannot be authorized because a security label is required

System Action: RACF denies the requested access.

User Response: Log on (or submit the job again) under an appropriate security label and try the access again. For a list of security labels you can specify, enter the following RACF command:

SEARCH CLASS(SECLABEL)

To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

**ICH408I INSUFFICIENT SECURITY
LEVEL/CATEGORY AUTHORITY**

Explanation: This error occurs when RACF detects an unauthorized attempt to access a RACF-protected resource.

System Action: RACF denies the requested access.

User Response: Enter the LISTUSER command to determine the security level and category or see your RACF security administrator.

**ICH408I LOGON/JOB INITIATION - EXCESSIVE
PASSWORDS OR INACTIVE USER**

Explanation: A user attempted to log on or submit a job too many times, or a user has not logged on or submitted a job for so long that the user ID has become inactive.

System Action: RACF prevents the user from logging on or the job from executing.

User Response: Report the exact text of this message to your RACF security administrator.

ICH408I

ICH408I LOGON/JOB INITIATION - INSUFFICIENT SECURITY LABEL AUTHORITY

Explanation: This message is issued when RACF detects an attempt to log on or submit a job with a missing or inappropriate security label. This could be issued on SETROPTS MLS when dominance check has failed or when the SETROPTS MLACTIVE option is in effect requiring a SECLABEL to be specified.

System Action: RACF prevents the user from logging on or the job from executing.

User Response: Log on (or submit the job again) under an appropriate security label. For a list of security labels you can specify, see your RACF security administrator.

Note: If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

SEARCH CLASS(SECLABEL)

ICH408I LOGON/JOB INITIATION - INVALID GROUP

Explanation: A user attempted to log on or submit a job with an unacceptable group ID specified. The group ID could be a translated group ID.

System Action: RACF prevents the user from logging on or the job from executing.

User Response: Correct any spelling errors in the group ID and try again. If you cannot remember the correct group ID, ask your RACF security administrator to provide you with a valid group ID.

ICH408I LOGON/JOB INITIATION - INVALID OIDCARD

Explanation: A user attempted to log on with an incorrect operator identification card.

System Action: RACF prevents the user from logging on.

User Response: Attempt to log on again. If the problem persists, report this message to your RACF security administrator.

ICH408I LOGON/JOB INITIATION - INVALID PASSWORD

Explanation: A user attempted to log on or submit a job using a password that is not valid or belongs to a protected user ID.

System Action: RACF prevents the user from logging on or the job from executing.

User Response: Correct any spelling errors in the

password and try again. If you cannot remember your password, ask your RACF security administrator to provide you with a new password.

ICH408I LOGON/JOB INITIATION - INVALID PASSWORD ENTERED AT TERMINAL *terminal-id*

Explanation: A user attempted to log on with a password that is not valid or belongs to a protected user ID. The attempt was made from terminal *terminal-id*.

System Action: RACF prevents the user from logging on.

User Response: Correct any spelling errors in the password and try again. If you cannot remember your password, ask your RACF security administrator to provide you with a new password.

ICH408I LOGON/JOB INITIATION - NOT AUTHORIZED TO APPLICATION

System Action: RACF prevents the user from logging on or the job from executing.

User Response: Report the exact text of this message to your RACF security administrator.

ICH408I LOGON/JOB INITIATION - NOT AUTHORIZED TO SECURITY LABEL

Explanation: You cannot use a particular security label (either for logging on or for initiating a job) unless you have at least READ access authority to the SECLABEL profile of that name.

System Action: RACF prevents the user from logging on or the job from executing.

User Response: Correct any spelling errors in the security label and try again.

Note: If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

SEARCH CLASS(SECLABEL)

Security Administrator Response: If the user should be allowed to use the indicated security label, give the user READ access authority to the SECLABEL profile. For example:

```
PERMIT security-label CLASS(SECLABEL)  
ID(userid) ACCESS(READ)
```

ICH408I LOGON/JOB INITIATION - NOT AUTHORIZED TO SUBMIT JOB *job-name*.

Explanation: A job was submitted with the indicated job name, and a check of the submitter user ID done

against the JESJOBS profile
 SUBMIT.xnode.jobname.userid failed, indicating that you
 are not authorized to submit jobs with the indicated job
 name, to run on the execution node (xnode), for the
 specified user ID. You do not have the appropriate
 access authority to a profile in the JESJOBS class.

System Action: RACF prevents the job from
 executing.

User Response: Correct any spelling errors in the job
 name and try again.

**ICH408I LOGON/JOB INITIATION - NOT
 AUTHORIZED TO {class-name
 entity-name} | TERMINAL/CONSOLE }**

Explanation: A user has attempted to:

- log on to the system,
- submit a job,
- perform a transaction, or
- in general, cause some unit of work to be initiated
 from a RACF defined port of entry,

and is not authorized to do so. *Class-name* is the port
 of entry class, such as TERMINAL or JESINPUT, and
entity-name is the port to which the user is not
 authorized, such as a particular terminal or JES node.
 See *z/OS Security Server RACF Data Areas*, for a list of
 the RACF port of entry classes and a mapping of the
 RUTKN data area.

Possible causes of this message are:

1. SECLABEL authorization mismatch
2. User or group authorization insufficient for terminal
3. Access is through universal access authority but
 NOTERMUACC specified for the connect group
4. Day-of-week or time failure caused by the terminal
 profile or the user profile

There is extended information on determining the cause
 of authorization failures in the *z/OS Security Server
 RACF Security Administrator's Guide* in the appendix
 section about "Debugging Problems in the RACF
 Database". For terminal related problems, refer to the
 section of that appendix that discusses "Authorizing
 Access to RACF-Protected Terminals".

The original TERMINAL/CONSOLE format of the
 message is used only when a token is not provided on
 the request. This format would most likely be issued
 only on an MVS release prior to MVS 3.1.3, where
 tokens are not supported, for the case where the user is
 trying to log on from a terminal to which he is not
 authorized.

System Action: RACF prevents access to the system
 from the named port of entry.

User Response: See your system administrator about
 obtaining authorization to a specific port of entry.

**ICH408I LOGON/JOB INITIATION - REVOKED
 USER ACCESS ATTEMPT**

Explanation: A user who has been revoked has
 attempted to log on or submit a job.

System Action: RACF prevents the user from logging
 on or the job from executing.

User Response: Report this message to your RACF
 security administrator.

**ICH408I LOGON/JOB INITIATION - SECURITY
 LABELS NOT COMPATIBLE.**

Explanation: Different security labels are associated
 with the submitter and the job and neither one
 dominates the other.

System Action: RACF prevents the job from
 executing.

User Response: Ensure that you are using the correct
 security labels for your logon session and job
 submission.

**ICH408I LOGON/JOB INITIATION - SUBMITTER
 IS NOT AUTHORIZED BY USER**

Explanation: You do not have the appropriate access
 authority to a profile in the SURROGAT class.

System Action: RACF prevents the user from logging
 on or the job from executing.

User Response: Do one of the following:

- If you do not intend to submit a job for another user,
 ensure that the USER parameter on the JOB
 statement specifies the user ID that you logged on
 with.
- If you do intend to submit a job for another user, ask
 the user whose job you are submitting to ensure that
 you have the appropriate access authority to his or
 her profile in the SURROGAT class. The following
 command can be used to do this:

```
RLIST SURROGAT userid.SUBMIT
AUTHUSER
```

where *userid* is the other user's (job owner's) user ID.

**ICH408I LOGON/JOB INITIATION SUBMITTER IS
 NOT AUTHORIZED TO SECURITY
 LABEL**

Explanation: Submitter does not have authorization to
 the SECLABEL required to run the job. You cannot use
 a particular security label (either for logging on or for
 initiating a job) unless you have at least READ access
 authority to the SECLABEL profile of that name.

Note: Both user (owner) and submitter of the job must
 be authorized to security label.

ICH408I

System Action: RACF prevents the job from executing.

User Response: Correct any spelling errors in the security label and try again.

Note: If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

ICH408I LOGON/JOB INITIATION - SURROGAT CLASS IS INACTIVE

Explanation: You cannot submit jobs on behalf of another user, because the SURROGAT class is inactive.

System Action: RACF prevents the job from executing.

User Response: Do one of the following:

- If you do not intend to submit a job for another user, ensure that the USER parameter on the JOB statement specifies the user ID that you logged on with.
- If you do intend to submit a job for another user, ask your RACF security administrator to activate the SURROGAT class.

ICH408I LOGON/JOB INITIATION - SYSTEM NOW REQUIRES MORE AUTHORITY

Explanation: The SETROPTS MLQUIET command has been issued. Jobs cannot be initiated, and users cannot logon, until the SETROPTS NOMLQUIET command is issued.

System Action: Unless the user is trusted, has the SPECIAL attribute, or is the console operator, RACF prevents the user from logging on or the job from executing.

User Response: Submit your job or attempt to log on again at a later time. If the problem persists, report this message to your RACF security administrator.

ICH408I LOGON/JOB INITIATION - USER AT TERMINAL(*terminal-id*) NOT RACF-DEFINED

Explanation: A user who does not have a RACF user profile has attempted to log on to the system.

System Action: RACF prevents the user from logging on.

ICH408I LOGON/JOB INITIATION - WARNING: INSUFFICIENT SECURITY LABEL AUTHORITY

Explanation: This error occurs when a user is logging on or a batch job is being initiated, and RACF detects

an unauthorized attempt to access a resource that has a security label associated with it. It is issued when MLS WARN is specified, and means that you would have failed a dominance check. For example, this message could be issued if a user attempts to log on at a RACF-protected terminal, and the profile protecting the terminal has a security label specified for it.

System Action: RACF allows the request to complete.

User Response: If the security label is misspelled, try again. If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

ICH408I LOGON/JOB INITIATION - WARNING: NOT AUTHORIZED TO SECURITY LABEL

Explanation: RACF issues this message when, for example, a user with the SPECIAL attribute specifies a security label such as SYSHIGH to which he or she does not have at least READ access authority.

System Action: RACF allows the user to log on or the job to execute.

ICH408I LOGON/JOB INITIATION - WARNING: SECURITY LABEL MISSING

Explanation: RACF issues this message when a security label is missing from one of the following:

- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

and the SETROPTS MLACTIVE(WARNING) option is in effect.

System Action: RACF allows the user to log on or the job to execute.

User Response: If a security label is not specified for the profile before the installation puts the SETROPTS MLACTIVE(FAILURES) option into effect, you will not be able to log on or submit the job.

ICH408I LOGON/JOB INITIATION - WARNING SECURITY LABELS NOT COMPATIBLE.

Explanation: Different security labels are associated with the submitter and the job and neither one dominates the other.

System Action: RACF allows the job to execute.

User Response: If you can specify security labels,

ensure that you are using the correct security labels for your logon session and job submission. If the system is not in COMPATMODE, this job will fail.

**ICH408I NETWORK JOB ENTRY - JOB FROM
NODE *node-name* NOT AUTHORIZED**

Explanation: The execution node is protected by the indicated profile in the NODES class (NJE processing). The submitting node or user ID is either not defined to or is not authorized to run on the execution node. The USER and GROUP indicated in the message are the user ID and group ID under which the job was to run (as translated by a profile in the NODES class).

**ICH408I NOT AUTHORIZED TO DEREGISTER
DIGITAL CERTIFICATES**

Explanation: A user attempted to deregister a digital certificate and is not authorized to do so.

System Action: InitACEE processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.DIGTCERT.DELETE profile is defined in the FACILITY class.
- Make sure the user has sufficient authority to the IRR.DIGTCERT.DELETE profile.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function profiles.

**ICH408I NOT AUTHORIZED TO EXPORT
DIGITAL CERTIFICATES**

Explanation: A user attempted to retrieve a digital certificate using the R_PKIServ callable service function EXPORT, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.EXPORT resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.EXPORT resource is defined in the FACILITY class.
- Make sure the user has sufficient authority to both of these resources.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

**ICH408I NOT AUTHORIZED TO GENERATE
DIGITAL CERTIFICATES**

Explanation: A user attempted to create a digital certificate using the R_PKIServ callable service function GENCERT, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.GENCERT resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.GENCERT resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.ADD resource is defined in the FACILITY class.
- Make sure the user has sufficient authority to all of these resources.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

**ICH408I NOT AUTHORIZED TO REQUEST
DIGITAL CERTIFICATES**

Explanation: A user attempted to request a PKI Services digital certificate using the R_PKIServ callable service function REQCERT, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.REQCERT resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.REQCERT resource is defined in the FACILITY class.
- Make sure the user has sufficient authority to all of these resources.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I

ICH408I NOT AUTHORIZED TO VERIFY DIGITAL CERTIFICATES

Explanation: A user attempted to verify a existing PKI Services digital certificate using the R_PKIServ callable service function VERIFY, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.VERIFY resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.VERIFY resource is defined in the FACILITY class.
- Make sure the user has sufficient authority to all of these resources.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO REVOKE DIGITAL CERTIFICATES

Explanation: A user attempted to revoke a PKI Services digital certificate using the R_PKIServ callable service function REVOKE, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.REVOKE resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.REVOKE resource is defined in the FACILITY class.
- Make sure the user has sufficient authority to all of these resources.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO GENERATE RENEWAL DIGITAL CERTIFICATES

Explanation: A user attempted to generate a PKI Services digital certificate as a renewal for an existing certificate using the R_PKIServ callable service function

GENRENEW, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.GENRENEW resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.GENRENEW resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.GENCERT resource is defined in the FACILITY class
- Make sure the user has sufficient authority to all of these resources

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO REQUEST THE RENEWAL OF DIGITAL CERTIFICATES

Explanation: A user attempted to request the renewal of an existing PKI Services digital certificate using the R_PKIServ callable service function REQRENEW, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.REQRENEW resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.REQRENEW resource is defined in the FACILITY class.
- Make sure the user has sufficient authority to all of these resources.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I INCORRECT PASS PHRASE SPECIFIED FOR DIGITAL CERTIFICATE EXPORT

Explanation: A user attempted to retrieve a PKI Services digital certificate using the R_PKIServ callable service function EXPORT, but provided an incorrect Certificate ID/pass phrase combination.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: Check that you have provided the correct Certificate ID and pass phrase for the certificate you are trying to export.

ICH408I INCORRECT CERTIFICATE SPECIFIED FOR VERIFICATION

Explanation: A user attempted to verify a digital certificate using the R_PKIServ callable service function VERIFY. The attempt failed because the certificate supplied is not known to PKI Services.

System Action: R_PKIServ processing ends. The certificate is not eligible for renewal or revocation by PKI Services.

User Response: Check that you have provided the correct certificate for verification. If using a web browser, close all browser windows and restart browser before trying again.

ICH408I NOT AUTHORIZED TO ADMINISTER DIGITAL CERTIFICATES OR CERTIFICATE REQUESTS. [READ|UPDATE] DENIED

Explanation: A user attempted to either query (READ) or modify (UPDATE) one or more PKI Services issued certificates or certificate requests using R_PKIServ callable service, but is not authorized to do so.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.RPKISERV.PKIADMIN resource is defined in the FACILITY class.
- Make sure the user has sufficient authority to this resource, READ or UPDATE.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO REGISTER DIGITAL CERTIFICATES

Explanation: A user attempted to register a digital certificate and is not authorized to do so.

System Action: InitACEE processing ends. RACF prevents the request from completing.

User Response: See your security administrator.

RACF Security Administrator Response: Do the following:

- Make sure the FACILITY class is active.
- Make sure the IRR.DIGTCERT.ADD profile is defined in the FACILITY class.
- Make sure the user has sufficient authority to the IRR.DIGTCERT.ADD profile.

See *z/OS Security Server RACF Security Administrator's Guide* for additional information on the IRR.DIGTCERT.function profiles.

ICH408I OMVS SEGMENT INCOMPLETELY DEFINED

Explanation: An attempt was made to dub a process and the OMVS segment in the current user's USER profile has no z/OS UNIX user identifier (UID) assigned or the profile for the user's current group does not have an z/OS UNIX group identifier (GID) assigned.

System Action: RACF returns an error return code to the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See *z/OS UNIX System Services Programming: Assembler Callable Services Reference* to determine the action of the syscall functions.

Programmer Response: Provide appropriate information about the failure to the user of your program, based on the function invoked and the return codes received.

ICH408I OMVS SEGMENT NOT DEFINED

Explanation: This error occurs when an attempt is made to dub a process and the current user's USER profile cannot be found in the RACF database or the profile has no OMVS segment.

System Action: RACF returns an error return code to the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See *z/OS UNIX System Services Programming: Assembler Callable Services Reference* to determine the action of the syscall functions.

Programmer Response: Provide appropriate information about the failure to the user of your program, based on the function invoked and the return codes received.

ICH408I PARTIAL VIOLATION ON COMMAND command

Explanation: This error occurs when RACF detects an unauthorized attempt to use a RACF command that would modify profiles on the RACF database.

ICH408I

**ICH408I PROFILE NOT FOUND. IT IS
REQUIRED FOR AUTHORIZATION
CHECKING.**

Explanation: A profile was not found for the general resource, and that general resource's class has a default return code greater than 4.

User Response: Ensure that a profile is created in the general resource class for the resource name indicated in the message before requesting access.

**ICH408I PROFILE NOT FOUND. RACFIND WAS
SPECIFIED ON THE MACRO.**

Explanation: This error occurs when RACF detects an attempt to access a resource that is not protected by a RACF profile, and RACFIND=YES was specified on the RACROUTE REQUEST=AUTH macro.

User Response: Ensure that a profile is created to protect this resource, in the class indicated in the message, before requesting access.

**ICH408I REMOTE JOB ENTRY - JOB FROM
NODE *node-name* NOT AUTHORIZED**

Explanation: A job submitted from the indicated node was not authorized to run on this system. (A UACC of NONE was specified on the NODES profile that applies to this node.)

ICH408I RENAME - GROUP NOT DEFINED

Explanation: This error occurs when RACF detects an unacceptable attempt to rename a resource.

System Action: RACF prevents the request from completing.

User Response: Correct any spelling errors in the group ID and try again. If you cannot remember the correct group ID, ask your RACF security administrator to provide you with a valid group ID.

ICH408I RENAME - INSUFFICIENT AUTHORITY

Explanation: This error occurs when RACF detects an unauthorized attempt to rename a resource.

System Action: RACF prevents the request from completing.

**ICH408I RENAME - NEW NAME ALREADY
DEFINED**

Explanation: This error occurs when RACF detects an improper attempt to rename a resource.

System Action: RACF prevents the request from completing.

**ICH408I RENAME - RESOURCE NOT
PROTECTED**

Explanation: RACF detected an attempt to access a data set that is not protected by a RACF profile, and RACROUTE REQUEST=AUTH is issued for the DATASET class when the SETROPTS PROTECTALL(FAILURES) option is in effect.

System Action: RACF fails the request.

User Response: Ensure that a profile is created in the DATASET class for the data set indicated in the message before requesting access.

**ICH408I RENAME - USER NOT MEMBER OF
GROUP**

Explanation: This error occurs when RACF detects an unauthorized attempt to rename a resource.

System Action: RACF prevents the request from completing.

User Response: Correct any spelling errors in the group ID and try again. If you cannot remember the correct group ID, ask your RACF security administrator to provide you with a valid group ID.

ICH408I RENAME - USER NOT RACF-DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to rename a resource.

System Action: RACF prevents the request from completing.

**ICH408I RENAME - WARNING: RESOURCE NOT
PROTECTED**

Explanation: This error occurs when RACF detects an unauthorized attempt to rename a resource.

System Action: RACF allows the request to complete.

ICH408I RESOURCE NOT PROTECTED

Explanation: This error occurs when RACF detects an unauthorized attempt to access a resource, but the resource is not protected.

System Action: RACF allows the requested access.

**ICH408I SECURITY LABEL MISSING FROM
USER, JOB, OR PROFILE**

Explanation: RACF issues this message when a security label is missing from one of the following:

- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

System Action: RACF denies the requested access.

User Response: If a line of this message indicates a profile in a RACF class, such as SMITH.CLIST CL(DATASET) VOL(D58000), the indicated resource profile is missing a security label.

ICH408I WARNING: DATA SET NOT CATALOGED

Explanation: This error occurs when the SETROPTS CATDSNS(WARNING) option is in effect, and RACF detects an unauthorized attempt to access an uncataloged data set.

System Action: RACF allows the requested access.

User Response: Catalog the data set and attempt the access again.

Note: If the SETROPTS CATDSNS(FAILURES) command is issued before the data set is cataloged, RACF will fail any subsequent access attempts.

ICH408I WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED

Explanation: This error occurs when RACF detects an unauthorized attempt to access a RACF-protected resource protected by a profile that is in WARNING mode.

System Action: RACF allows the requested access.

ICH408I WARNING: INSUFFICIENT SECURITY LABEL AUTHORITY

Explanation: This error occurs when the SETROPTS MLS(WARNING) option is in effect and RACF detects an attempt to access a resource that would fail because of the security label associated with the resource.

System Action: RACF allows the requested access.

User Response: Consider logging on again (or submitting the job again) with an appropriate security label. To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

Note: If the SETROPTS MLS(FAILURES) command is issued, RACF will fail any subsequent access attempts.

ICH408I WARNING: RESOURCE NOT PROTECTED

Explanation: This error occurs when RACF detects an unauthorized attempt to access an unprotected resource.

System Action: RACF allows the requested access.

ICH408I WARNING: SECURITY LABEL MISSING FROM USER, JOB, OR PROFILE

Explanation: RACF issues this message when a security label is missing from one of the following and the SETROPTS MLACTIVE(WARNING) option is in effect:

- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

System Action: RACF allows the requested access.

User Response: If a line of this message indicates a profile in a RACF class, such as SMITH.CLIST CL(DATASET) VOL(D58000), the indicated resource profile is missing a security label.

ICH409I *abend-code[-yy]* ABEND DURING request {PROCESSING | PARAMETER VALIDATION}

Explanation: A failure occurred during the RACF processing of the indicated request. If the request indicated in the message is RACROUTE REQUEST=VERIFY, REQUEST=AUTH, REQUEST=DEFINE, or REQUEST=LIST, RACF was processing the SVC related to the request. If the request indicated in the message is GENLIST, RACF was building in-storage generic profiles. If the request indicated in the message is DIRAUTH, RACF was processing a directed authorization check request. If the request indicated in the message is IRRSxx00, RACF was processing the indicated callable service.

System Action: RACF processing stops.

Operator Response: Report the exact text of this message to your system programmer or RACF security administrator, or both, and save the message output.

Programmer Response: See "Problem Determination."

Problem Determination: Try to determine where the abend occurred. RACF, a RACF caller, or other system processing could have caused the abend. If the message says PARAMETER VALIDATION, the RACF caller probably caused the abend.

If the last two digits of the abend are 82, 83, 84, 85, C6, or C7, locate the abend in Chapter 8, "RACF abend codes" on page 295. The abend description provide additional assistance.

If the last two digits of the abend are *not* 82, 83, 84, 85, C6, or C7, examine the abend code and analyze the error using general problem determination techniques. The value yy is the contents of Register 15 (in hexadecimal). For system abend and reason codes, see your system codes documentation.

ICH411I • ICH416I

Destination: Descriptor code is 1. Routing codes are 9 and 11.

ICH411I MAXIMUM PROFILE SIZE EXCEEDED.
profile-name **NOT ALTERED.**

Explanation: During RACF processing, an attempt was made to expand the profile indicated in the message. The profile has reached the maximum size that RACF can handle (65,535 bytes); the profile cannot be made larger.

System Action: Processing stops.

Operator Response: Report this message to the system programmer or the RACF security administrator, or both, and save this output.

Programmer Response: The profile has reached the maximum size allowed. If possible, decrease the size of the profile; if that is not possible, split the profile. For example, you could split a group with too many users into several smaller groups.

Destination: Descriptor code is 4. Routing code is 9.

ICH412I RACF DATA AREAS FORCED BELOW
THE 16-MEGABYTE LINE.

Explanation: RACF was unable to allocate storage above 16 megabytes because at least one of the installation exit routines does not support 31-bit addressing mode.

Operator Response: Notify system programmer.

Programmer Response: If possible, change the installation exit routines to support 31-bit addressing mode.

Destination: Descriptor code is 4. Routing code is 2.

ICH414I SMF IS RECORDING ON ITS LAST
AVAILABLE DATA SET. WHEN DATA
SET FILLS UP, SMF EXIT IEFU29 WILL
PLACE THE SYSTEM IN A WAIT
STATE.

Explanation: SMF exit routine IEFU29, which stops system operations when all SMF data sets are full, has been installed on your system. This exit routine helps ensure that no SMF data is lost.

System Action: Processing continues until the SMF data set fills up. At that time, SMF exit IEFU29 places the system in a wait state.

Operator Response: Using installation-defined procedures, archive the SMF data sets that are full. This makes them available for re-use.

Destination: Descriptor code is 2. Routing codes are 1, 2, and 9.

ICH415I session attempt rejected. reason code
= code, entity *netid.luid1.luid2*, **profile**
profile-name, **at** *hh:mm:ss* **on** *month*, *day*,
year

Explanation: An attempt by logical unit *netid.luid1* to establish a session with the logical unit *luid2* has been rejected for a security reason. The entity *netid.luid1.luid2* was covered by profile *profile-name*. The message is routed to the user specified in the NOTIFY field of the profile.

This message is identical to ICH70005I except that it is sent to the MVS security console.

System Action: The session ends.

Operator Response: Notify the RACF security administrator.

Problem Determination: Check the reason code in the message for one of the following values:

- | | |
|-----------|--|
| 02 | Local LU's session key will expire in five days or less |
| 03 | Partner LU's access has been revoked |
| 04 | Session key does not match partner LU session key |
| 05 | Partner LU stops the session due to a security reason |
| 06 | Partner LU verification required but no session key is defined on this system |
| 07 | Possible security attack by partner LU |
| 08 | Verification was not indicated by partner LU but a session key exists on this system |
| 09 | Verification was indicated by partner LU but a session key does not exist on this system |
| 10 | Failure due to SNA security related protocol error |
| 11 | Failure due profile change during verification |
| 12 | A profile was found with an expired session key |

Destination: Descriptor code is 4. Routing codes are 9 and 11.

ICH416I RACF DETECTED AN INVALID
NON-EGN DATASET PROFILE NAME.
PROFILE *profile-name* **DOES NOT**
PROTECT THE INTENDED
RESOURCES.

Explanation: RACF detected a profile that was added before the enablement of Enhanced Generic Names (EGN) and that cannot be interpreted as intended under EGN rules. This message identifies the non-EGN generic data set profile name. Under EGN rules, the profile may not protect the resources that it was defined

to protect. If this message is issued during processing of a SEARCH or LISTDSD GENERIC request, bad profile names (particularly names 43 and 44 characters in length) may also have been displayed and the output should be considered unreliable.

For example, suppose the following six generic data set profiles were defined before turning EGN on:

```
1 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.*'
2 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD*'
3 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*'
4 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD*'
5 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.D.*'
6 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD*'
```

Then EGN was enabled and three more generic data set profiles were defined:

```
7 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.**'
8 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.**'
9 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.**'
```

A subsequent SEARCH request would display the following:

```
SEARCH CLASS(DATASET)
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.

A IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.* (G)
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
B IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD.* (G)
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.
C IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.** (G)
D IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.* (G)
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
E IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD* (G)
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.
F IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.D.* (G)
G IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD* (G)
H IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD* (G)
I IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD* (G)
```

Because of RACF command processing, the ICH416I message may be issued more than once. However, any time it is issued during a command invocation, the command output must be considered unreliable. In the example above, changes in EGN rules caused RACF to incorrectly interpret non-EGN profiles (1) and (2) as SEARCH profiles (A) and (B). These profiles no longer cover the intended resources. Even though names (D) and (E) appear correct, with no additional characters at the end, they also do not cover the intended resources and cause ICH416I messages to be issued. EGN

profiles (7), (8), and (9) were correctly displayed by SEARCH as (C), (F), and (I). Profiles (G) and (H) follow the same rules under non-EGN and EGN, so they actually protect what they were intended to protect.

System Action: RACF processing of the request continues.

Operator Response: Report this message to the system programmer or the RACF security administrator and save the message output.

Programmer Response: See problem determination.

Problem Determination: This message identifies the bad profile.

An EGN profile, possibly less specific, can be defined to protect the desired resources; however the original bad non-EGN profile must still be deleted to prevent further ICH416I messages.

To delete bad profiles:

1. Use SETROPTS NOEGN to temporarily disable EGN. During this time, there should be no other system activity, in order to prevent the creation of generic profiles that could result in additional problems. Under normal circumstances, it is not recommended that EGN be turned off after it is turned on.
2. Use SEARCH GENERIC CLIST NOMASK NOLIST to create a CLIST containing generic data set profile names.
3. Edit the CLIST to find 42- and 43-character names ending in '*'.
4. Delete the profiles found.
5. Use SETROPTS EGN to re-enable EGN.
6. Define profiles according to EGN rules that protect the resources intended to be protected by the non-EGN profile names.

Destination: Descriptor code is 4. Routing codes are 9 and 11. Routing code 11 is only used when a TSO environment is not in effect.

ICH417I THE ENVIRONMENT IS NOT CONTROLLED. CONDITIONAL ACCESS LIST BYPASSED FOR DATA SET
dsname

Explanation: The profile that protects the data set has a conditional access list that would have granted access, but RACF did not use it because the environment is not controlled.

System Action: RACF denies the requested access.

User Response: Check for additional error messages describing the reason the environment is not controlled and take appropriate action to ensure the environment is controlled.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH418I **CONDITIONAL ACCESS LIST FOR DATA SET *dsname* DID NOT GRANT AUTHORITY TO PROGRAM(S):**
program-name1, program-name2,
program-name3 ...

Explanation: The profile protecting the data set has a conditional access list, but it did not contain the correct program or programs on the access list to grant authority to the data set. Either:

1. *program-name1* is the currently executing program and does not appear in the conditional access list; or
2. one or more programs defined to the PROGRAM class with PADCHK are present in the environment, and do not appear in the conditional access list of the profile protecting the data set. Only the first 14 programs found are listed in the message.

If a program name reads *EXEFILE, the program is an executable file that was loaded from the Hierarchical File System (HFS) and is not available to RACF.

System Action: RACF denies the requested access.

User Response: Issue the PERMIT command to place the necessary program(s) on the conditional access list of the profile covering the data set, or ask your security administrator to do so.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH419I **THE ENVIRONMENT IS NOT CONTROLLED. ATTEMPT TO LOAD PROGRAM *program-name* FROM LIBRARY *dsname* FAILED.**

Explanation: The profile in the PROGRAM class that protects *program-name* gives you only EXECUTE authority. You tried to use this program in an uncontrolled environment or address space. This is not allowed. Or, you currently have an execute-controlled library open, and you tried to load a program that is not controlled.

System Action: RACF denies the requested access.

User Response: Check for additional error messages describing the reason the environment is not controlled and take the appropriate action to ensure the environment is controlled. If this program is not controlled, then close the execute-controlled library that is currently open, or ask your security administrator to change your access to the library to READ.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH420I **PROGRAM *program-name* [FROM LIBRARY *dsname*] CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED.**

Explanation: You have previously loaded *program-name* into your environment. This program is not protected by a RACF profile in the PROGRAM class. The presence of this program has caused the environment to be marked uncontrolled.

User Response: Try to access this resource in an environment that does not contain *program-name*. If this is not possible, report the message to your security administrator.

RACF Security Administrator Response: Define a profile in the PROGRAM class to protect the program indicated by the message.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH421I **REASON FOR UNCONTROLLED ENVIRONMENT IS NOT KNOWN.**

Explanation: RACF cannot determine why the environment is not controlled. This indicates that a program marked the environment uncontrolled without using the environment service, IRRENS00.

User Response: If you are in a TSO/E environment, logoff and logon again or use TSOEXEC to create a new controlled environment, and then try to access this resource. If the problem continues, report the message to your security administrator.

RACF Security Administrator Response: Check PROGRAM class definitions and ensure the user should have access to the resource when accessing it as attempted. Report the problem to the IBM support center.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH422I **THE ENVIRONMENT CANNOT BECOME UNCONTROLLED.**

Explanation: The IRRENS00 service received a request to mark the environment uncontrolled. This request cannot be satisfied because the environment must remain controlled to maintain system security.

System Action: RACF denies the request.

User Response: Check for additional error messages describing the reason the environment cannot become uncontrolled and take the action specified for the additional messages. Or, try in a different environment that does not contain sensitive data or programs that require the environment to be kept controlled.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH423I RACF EXECUTE-CONTROLLED PROGRAMS ARE ACTIVE:
program-name1, program-name2,
program-name3 ...

Explanation: The IRRENS00 service received a request to mark the environment uncontrolled, and has determined that it cannot satisfy that request due to the presence of execute-controlled programs. Only the first 20 programs found are listed in the message.

If two ICH423I messages are received, then there are currently more than one execute-controlled programs active in the environment, and the environment was originally marked keep-controlled because of an execute-controlled program.

User Response: Report the message to your security administrator.

RACF Security Administrator Response: The user has attempted a function that would make his environment uncontrolled. RACF failed the request because there are execute-controlled programs running in his environment. Determine if the user should be allowed to perform this action in his current environment. If so, correct the RACF PROGRAM and DATASET class definitions to allow access.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH424I DATA SETS OPENED USING RACF WHEN(PROGRAM(...)) ARE STILL OPEN: *dsname1, dsname2, dsname3 ...*

Explanation: The IRRENS00 service received a request to mark the environment uncontrolled. It cannot satisfy that request because program-accessed data sets are already open in the environment. Only the first 4 data sets found are listed in the message.

User Response: Close the data sets listed in the message, and try again.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH425I UNIX SYSTEM SERVICES MUST KEEP THE ENVIRONMENT CONTROLLED.

Explanation: The IRRENS00 service received a request to mark the environment uncontrolled. It cannot satisfy that request because z/OS UNIX has requested the environment be kept controlled.

User Response: Check for additional error messages with the message prefix BPX describing the reason the environment cannot become uncontrolled and take the action specified for the additional messages. Or, try in a different environment that does not contain sensitive data or programs that require the environment be kept controlled.

Destination: Descriptor code is 6. Routing code is 9 and 11.

ICH426I NON-MAIN PROGRAM IS IN CONTROL. CONDITIONAL ACCESS LIST BYPASSED FOR DATA SET *dsname*

Explanation: The profile that protects the data set has a conditional access list that would have granted access via WHEN(PROGRAM), but RACF did not use it because ENHANCED PGMSECURITY mode is in effect (FACILITY profile IRR.PGMSECURITY exists with an APPLDATA value of ENHANCED) and the environment was established by a program that did not have the MAIN attribute.

System Action: Access is denied by RACF.

User or RACF Security Administrator Response:

Check for additional messages that provide further details, such as ICH428I. Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command or via IKJEFTSR service) has a specific PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, if it is a program that you trust to maintain the environment properly for using conditional access, or you may change the way you invoke the program (e.g. under TSO consider invoking the program via the TSOEXEC command), or you may change the system to run in BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of MAIN. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH427I NON-MAIN PROGRAM IS IN CONTROL. TEMPORARY USE OF CONDITIONAL ACCESS LIST ALLOWED FOR DATA SET *dsname*

Explanation: The profile that protects the data set has a conditional access list that would grant access via WHEN(PROGRAM) if BASIC PGMSECURITY was in effect. However, ENHANCED PGMSECURITY is in effect and the environment was established by a program that did not have the MAIN attribute. This would normally cause RACF to reject use of the conditional access list entry, but RACF has allowed it because the administrator enabled WARNING mode for ENHANCED PGMSECURITY. This access would have failed if the administrator had instead enabled ENHANCED mode of PGMSECURITY.

System Action: RACF allows the requested access, but issues the warning message.

User or RACF Security Administrator Response:

ICH428I • ICH430I

Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command or via IKJEFTSR service) has a PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, if it is a program that you trust to maintain the environment properly for using conditional access, or you may change the way you invoke the program (e.g. under TSO consider invoking the program via the TSOEXEC command), or you may change the option to BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of MAIN. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC.

Do not enable the failure mode of ENHANCED PGMSECURITY before you resolve this message, or you will cause accesses to fail.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH428I **PROGRAM** *program-name* **FROM** {
 library-name | **LPA** | **JPA** }
 ESTABLISHED THE CURRENT
 EXECUTION ENVIRONMENT

Explanation: The named program from the specified library (or from the Link Pack or Job Pack) was the first program executed in this jobstep or, if applicable, in this TSO service routine (IKJEFTSR, TSOEXEC) environment. This program is not defined to RACF as a MAIN program via a PROGRAM profile with an APPLDATA of MAIN and thus, in an ENHANCED PGMSECURITY environment, is not trusted to provide a safe environment for use of program access to data sets (PADS, or WHEN(PGM) conditional access list entries) for loading EXECUTE-controlled programs, nor for some UNIX System Services functions. RACF provides the name and location of the program to help you diagnose the problems reported in other messages issued by RACF or UNIX System Services.

System Action: None. Also, see other messages issued by RACF or UNIX System Services to see the system action that occurred.

User or RACF Security Administrator Response:

Examine the other messages you received and take the appropriate actions indicated for those messages.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH429I **NON-MAIN PROGRAM IS IN CONTROL.**
 ATTEMPT TO LOAD PROGRAM
 program-name **FROM LIBRARY**
 library-name **FAILED.**

Explanation: The user has only EXECUTE authority to the named program, via the PROGRAM profiles or

the DATASET profile for the library. RACF cannot allow use of the program because ENHANCED PGMSECURITY mode is in effect (FACILITY profile IRR.PGMSECURITY exists with an APPLDATA value of ENHANCED) and the environment was established by a program that did not have the MAIN attribute.

System Action: Access is denied by RACF.

User or RACF Security Administrator Response:

Check for additional messages that provide further details, such as ICH428I. Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command or via IKJEFTSR service) has a specific PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, if it is a program that you trust to maintain the environment properly for using conditional access, or you may change the way you invoke the program (e.g. under TSO consider invoking the program via the TSOEXEC command), or you may change the system to run in BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of MAIN. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH430I **NON-MAIN PROGRAM IS IN CONTROL.**
 TEMPORARY USE OF PROGRAM
 program-name **FROM LIBRARY**
 library-name **ALLOWED.**

Explanation: The user has only EXECUTE authority to the named program, via the PROGRAM profiles or the DATASET profile for the library, and ENHANCED PGMSECURITY mode is in effect (FACILITY profile IRR.PGMSECURITY exists with an APPLDATA value of ENHANCED) and the environment was established by a program that did not have the MAIN attribute. This would normally cause RACF to prohibit use of the program by this user, but RACF has allowed it because the administrator enabled the WARNING mode for ENHANCED PGMSECURITY. This access would have failed if the administrator had instead enabled the ENHANCED mode of PGMSECURITY.

System Action: RACF allows the requested access, but issues the warning message.

User or RACF Security Administrator Response:

Check for additional messages that provide further details, such as ICH428I. Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command or via IKJEFTSR service) has a PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, if it is a program that you trust to maintain

the environment properly for using conditional access, or you may change the way you invoke the program (e.g. under TSO consider invoking the program via the TSOEXEC command), or you may change the option to BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of MAIN. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC.

Do not enable the failure mode of ENHANCED PGMSECURITY before you resolve this message, or you will cause accesses to fail.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

RACF initialization messages

ICH500I **I/O ERROR DURING RACF
INITIALIZATION [{PRIMARY | BACKUP }
RACF DATA SET SEQUENCE *nnn*,
dsname]**

Explanation: During RACF initialization, an I/O error occurred on the RACF database.

System Action: The system issues ICH502A following this message, then waits for the operator's reply.

Operator Response: Notify your system programmer.

Programmer Response: Determine if the device or volume used for the RACF database is functioning properly.

Destination: Descriptor code is 4. Routing code is 2.

ICH501I **--RACF IS NOT ACTIVE.--**

Explanation: During RACF initialization or sysplex communication processing, either a RACF error or a system error occurred.

System Action: RACF becomes inactive. If RACF had joined the sysplex data sharing group, it leaves the group. RACF allows access to the following:

- Resources accessed by started tasks that are marked as privileged or trusted in the RACF started procedures table (ICHRIN03)
- A user's own data sets
- Any other data sets to which the operator allows access
- Any general resource for which the access authorization is done via RACHECK, and to which the operator allows access
- All general resources for which the access authorization is done via RACROUTE REQUEST=AUTH

Operator Response: Notify your system programmer.

Programmer Response: Correct the problem and IPL again.

Problem Determination: A message (either ICH505A, ICH564A, ICH565A, ICH566A, ICH567A, ICH568A, ICH569A, ICH570A, ICH571A, ICH572A, ICH573A, ICH574A, ICH575A, or ICH576A) precedes this message if the error occurred during initialization and indicates the cause of the error. For sysplex communication errors, there is an abend and an associated dump.

Note: In previous releases, the following messages preceded this message: ICH511I, ICH512I, ICH517I, ICH518I, ICH519I, ICH523I, ICH526I, ICH528I, ICH537I, ICH549I, ICH550I, ICH551I, or ICH553I.

Destination: Descriptor code is 2. Routing code is 1.

ICH502A **SPECIFY NAME FOR {PRIMARY |
BACKUP} RACF DATA SET SEQUENCE
nnn OR 'NONE'**

Explanation: The data set name table (ICHRDSNT) indicates that a primary (or backup) database is requested for the sequence number *nnn*. However, either no data set name was given in the table or an error occurred while the data set was being processed. In the latter case, a message (either ICH500I, ICH503I, ICH506I, ICH507I, ICH510I, or ICH515I) precedes this message.

System Action: The system waits for the operator's reply.

Operator Response: Specify either the name of an alternate RACF database or NONE if no primary (or backup) RACF database is to be used for this sequence number.

Notes:

1. If an alternate database is specified, it must be online and cataloged.
2. If there is a problem with the primary RACF database, and RACF issues message ICH510I and ICH502A, you might (appropriately) reply to ICH502A with the name of the backup RACF database. RACF attempts to allocate the backup database as the primary database. If, following specifications in the data set name table, RACF then attempts to allocate the backup RACF database as the backup database, RACF will issue message ICH515I, then ICH502A again. This is normal, and you should consult with your system programmer about whether to reply with NONE or the name of yet another RACF database.

Programmer Response: See "Problem Determination."

Problem Determination: Be sure the RACF database is cataloged and online, and that the device on which the RACF database is mounted is functioning properly. If the database was updated by the IRRMIN00 utility, ensure that templates of the correct level were added to the RACF database. (Down-level templates can cause a RACF manager error.)

Destination: Descriptor code is 2. Routing code is 1.

ICH503I **RACF DATA SET NOT FOUND
[{PRIMARY | BACKUP } RACF DATA
SET SEQUENCE *nnn*, *dsname*]**

Explanation: During initialization, or the processing of a propagated RVAR ACTIVE command, the RACF database could not be found.

System Action: The system issues ICH502A following this message, then waits for the operator reply. If the system is enabled for sysplex communication and it is not the first system to IPL, message ICH502A is not issued and processing continues.

Operator Response: Notify your system programmer.

Programmer Response: Ensure that the correct RACF database is specified in MSTRJCL or that it is included in the operator's reply to message ICH502A. Ensure that it is cataloged and online.

System Programmer Response: If this message is received during the processing of a propagated RVARY ACTIVE command on a SYSPLEX, (**DATASHARING or SYSPLEX COMMUNICATION**), and is followed by messages ICH529I and ICH532I, verify that the RACF DS named in ICH503I is cataloged on the same volume as the RACF DS of the same name on the member of the SYSPLEX on which the RACF RVARY ACTIVE command was entered. If the volume ids are not the same, recatalog the RACF DS to be on the same volume as the system on which the RVARY command was entered.

Destination: Descriptor code is 4. Routing code is 2.

ICH504I USER ATTRIBUTE DATA SET NOT FOUND

Explanation: During RACF initialization, the TSO UADS data set could not be found. The UADS data set had been defined in MSTRJCL.

System Action: The system continues with the IPL, but TSO/E is not usable until the next IPL.

Operator Response: Report this message to the system programmer.

Programmer Response: If you want to use TSO/E before the next *scheduled* IPL, you need to manually re-IPL the system to activate TSO/E.

Problem Determination: Ensure the TSO UADS data set is cataloged and online.

Destination: Descriptor code is 4. Routing code is 2.

ICH505A RACF INITIALIZATION ABEND S 'xxx'

Explanation: A system abend occurred during RACF initialization. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: See "Problem Determination."

Problem Determination: See Chapter 8, "RACF abend codes" on page 295 for system completion code xxx. The SDUMP data set and LOGREC data provide other diagnostic information. Correct the error and IPL again.

Destination: Descriptor codes are 1 and 2. Routing code is 1.

**ICH506I RACF DATA SET CANNOT BE USED
[PRIMARY | BACKUP } RACF DATA
SET SEQUENCE *nnn, dsname*]**

Explanation: The data set is not usable as a RACF database for one of the following reasons:

- The ICB indicates that the data set has been extended.
- The data set was used as input in the IRRUT400 utility with the LOCKINPUT parameter specified.
- The initialization of the RACF database failed.

Note: If this message is issued with either message ICH560I or ICH561I, refer to the information for those messages.

System Action: The system issues ICH502A following this message, then waits for the operator's reply.

Operator Response: Notify your system programmer.

Programmer Response: Ensure that the correct RACF database is specified in MSTRJCL or that it is included in the operator's reply to message ICH502A.

Destination: Descriptor code is 4. Routing code is 2.

**ICH507I RACF DATA SET NOT AT CURRENT
RELEASE LEVEL [PRIMARY |
BACKUP } RACF DATA SET
SEQUENCE *nnn, dsname*]**

Explanation: The primary or backup RACF database being used is not at the appropriate release level.

System Action: The system issues ICH502A following this message, then waits for the operator's reply.

Operator Response: Check the response to message ICH502A. It should be the name of a RACF database at the current release level. If this message recurs, report this message (and the response to message ICH502A) to the system programmer.

Programmer Response: See "Problem Determination" for message ICH502A.

Destination: Descriptor code is 4. Routing code is 2.

**ICH508I ACTIVE RACF EXITS: {NONE |
name,...,name}**

Explanation: During RACF initialization, one or more of the following installation exit routines or tables indicated by *name* were loaded from LPA and are in effect for this IPL:

ICHCCX00
Command preprocessing exit

ICH509I • ICH510I

ICHCNX00

Command preprocessing exit

ICHDEX01

Password authentication exit

ICHDEX11

Password authentication exit

ICHNCV00

Naming conventions table

ICHWPX01

New-password processing exit

ICHRCX01

REQUEST=AUTH preprocessing exit

ICHRCX02

REQUEST=AUTH postprocessing exit

ICHRDX01

REQUEST=DEFINE preprocessing exit

ICHRDX02

REQUEST=DEFINE postprocessing exit

ICHRFX01

REQUEST=FASTAUTH preprocessing exit

ICHRFX02

REQUEST=FASTAUTH postprocessing exit

ICHRFX03

REQUEST=FASTAUTH preprocessing exit

ICHRFX04

REQUEST=FASTAUTH postprocessing exit

ICHRIX01

REQUEST=VERIFY preprocessing exit

ICHRIX02

REQUEST=VERIFY postprocessing exit

ICHR LX01

REQUEST=LIST pre/postprocessing exit

ICHR LX02

REQUEST=LIST selection exit

IRRACX01

ACEE compression and expansion

IRRACX02

ACEE compression and expansion

Note: This message only applies to exits during IPL.

System Action: RACF initialization continues.

Operator Response: Ensure that all of the expected exit routines are listed in this message.

Programmer Response: If any expected exit routines are not listed, the exits to be loaded must be link-edited into an LPA library with the appropriate names.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH509I

SYSRACF DD STATEMENT NOT SPECIFIED IN MSTRJCL OR ALLOCATION FAILURE FOR RACF DATA SET.

Explanation: One of the following occurred:

- RACF could not find SYSRACF (a DD statement) in MSTRJCL.
- RACF could not find the RACF database in the data set name table (ICHRDSNT).
- Dynamic allocation could not allocate the RACF database. SYSRACF might be in the MSTRJCL but the RACF data set might not be cataloged in the proper volume.

System Action: The system issues ICH502A following this message, then waits for the operator's reply. If the system is enabled for sysplex communication and it is not the first system to IPL, message ICH502A is not issued and processing continues.

Operator Response: Notify your system programmer.

Programmer Response: See "Problem Determination."

Problem Determination: If SYSRACF has been removed from the MSTRJCL, check to see if the RACF database has been placed in the data set name table (ICHRDSNT). If not, correct the error and IPL again.

If the SYSRACF DD statement is present in MSTRJCL, the RACF database has been cataloged in the wrong volume. Catalog SYSRACF and IPL again.

Destination: Descriptor code is 4. Routing code is 2.

ICH510I

ALLOCATION FAILED FOR RACF DATA SET [{PRIMARY | BACKUP } RACF DATA SET SEQUENCE *nnn*, *dsname*]

Explanation: The attempt to dynamically allocate the database specified has failed.

System Action: If this message is received during RACF initialization, it is followed by message ICH502A to prompt the operator for another data set name for the data set sequence number *nnn*. If the system is enabled for sysplex communication and it is not the first system to IPL, message ICH502A is not issued and processing continues.

If this message is received during an RVAR request, message ICH502A is not issued and the RVAR command retries the activation of the data set.

Operator Response: Notify the system programmer.

System Programmer Response: If this message is received during RACF initialization, verify that the name specified is a valid RACF data set name. If the specified name is correct, make sure that the device containing the data set is on line and available. Instruct the operator to reply to message ICH502A with the same data set name. If the specified name is incorrect,

provide the operator with the correct RACF data set name for the data set sequence number *nnn*. The operator uses this name to reply to message ICH502A. Correct any errors in the data set name table.

If this message is received during the initialization of RACF on a system attempting to join a SYSPLEX, **(DATASHARING or SYSPLEX COMMUNICATION)**, and is followed by message ICH501I, verify that the RACF DS named in ICH510I is cataloged on the same volume as the RACF DS of the same name on the current members of the SYSPLEX. If the volume ids are not the same, recatalog the RACF DS to be on the same volume as the current members of the SYSPLEX.

If this message is received during an RVARY request, make sure that the specified RACF data set is cataloged and the device containing the data set is on line and available. Reissue the RVARY command.

Destination: Descriptor code is 4. Routing code is 2.

**ICH511I RACF DETECTED AN ERROR IN THE
 {IBM SUPPLIED | INSTALLATION}
 CLASS DESCRIPTOR TABLE, ENTRY
 entry-name, ERROR CODE yy**

Explanation: RACF encountered an error for entry *entry-name* in either the installation-defined class descriptor table, ICHRRCDX, or the class descriptor table supplied by IBM, ICHRRCDX. The class descriptor table is located in one of the following:

- SYS1.LINKLIB
- A library concatenated to SYS1.LINKLIB
- LPA (for ICHRRCDX only)

This message is followed by message ICH501I. Error code *yy* identifies the problem as follows:

Code	Description of Error
1	The class name is less than 4 characters or contains embedded blanks or non-alphanumeric characters.
2	The ID field has a value of zero.
3	The POSIT mask has more than 1 bit turned on or has no bits turned on.
4	The field that defines the length of the class name (MAXLNTH or MAXLENX) has a value greater than 246.
5	The class is designated as a resource group class, but the MEMBER field does not contain a member class name.
6	The table contains more than 1024 entries.
7	Two entries have the same class names.
8	One of the following: <ul style="list-style-type: none"> • A grouped class specifies a member that does not exist in the table or is incorrect, or

a member class specifies a group that does not exist in the table or is incorrect.

- A pair of classes reference each other, but one or both is not a grouping class.

- | | |
|----|--|
| 9 | One of the reserved class names (USER, GROUP, or DATASET) appears in the class table. |
| 10 | An entry in the installation table has a class name with the same name as an entry in the table supplied by IBM. |
| 11 | The area reserved for the pointer to the RACLISTed profiles is not zero. |
| 12 | The area reserved for the pointer to the GENLISTed profiles is not zero. |
| 13 | The length of the class descriptor (CDT) entry (as indicated in a field in the entry itself) is not the same as the actual length of the class descriptor table entry. |

System Action: IPL continues.

Operator Response: Ensure that the system parameters MLPA and LNK have been specified properly. If they are not, correct any errors and IPL again. Otherwise, notify your system programmer.

Programmer Response: Ensure that no errors occurred during the assembly of the table entries, that the table was properly link-edited, and that modifications subsequent to link-edit did not cause an error. Correct the error and IPL again.

Destination: Descriptor code is 4. Routing code is 2.

**ICH512I RACF UNABLE TO LOCATE *modname*
 IN LPA**

Explanation: RACF encountered one of the following errors:

- RACF searched the link-pack area and could not locate one of the routines necessary for RACF processing. Processing cannot continue. Message ICH501I follows this message.
- RACF could not locate ICHRRF00 in the link-pack area. Processing continues, but the user cannot invoke RACF with the RACROUTE macro instruction.

System Action: IPL continues.

Operator Response: Ensure that the system parameters MLPA and LNK have been specified properly. If they are not, correct any errors and IPL again. Otherwise, notify your system programmer.

Programmer Response: If the system parameters MLPA and LNK have been properly specified, one of the following has happened:

- RACF has not been installed properly.

ICH513I • ICH518I

- The MLPA and LNK lists do not contain all the entries necessary to load the RACF-required modules into the link-pack area.
- There is an error in the link-edit of a required routine.

Correct the error and IPL again.

Destination: Descriptor code is 4. Routing code is 2.

ICH513I DATA SET NOT REFERENCED IN RANGE TABLE PRIMARY RACF DATA SET SEQUENCE *nnn, dsname*

Explanation: There are no entries in the range table that would allow access to the database indicated by *dsname* with sequence number *nnn*.

System Action: The database is not available to RACF.

Operator Response: Notify your system programmer.

System Programmer Response: Check for a mismatch between the data set name table (ICHRDSNT) and the range table (ICHRRNG).

Destination: Descriptor code is 4. Routing code is 2.

ICH515I DATA SET ALREADY IN USE AS A RACF DATA SET [{PRIMARY | BACKUP} RACF DATA SET SEQUENCE *nnn, dsname*]

Explanation: The data set *dsname* with sequence number *nnn* has already been allocated for use by RACF as a primary or backup database.

System Action: The system issues ICH502A following this message, then waits for the operator's reply.

Operator Response: Notify your system programmer.

Programmer Response: See "Problem Determination."

Problem Determination: Ensure that the data set name table (ICHRDSNT) does not contain two entries with the same database name. Also, ensure that the operator does not respond to message ICH502A with the name of a database that already exists in the data set name table.

Destination: Descriptor code is 4. Routing code is 2.

ICH516I UNABLE TO ESTABLISH RECOVERY ENVIRONMENT RACF INITIALIZATION CONTINUING.

Explanation: RACF issued an ESTAE macro instruction. A nonzero return code indicated that the system could not establish a recovery routine to get control if a RACF failure occurred.

System Action: RACF processing continues without active error recovery.

Operator Response: Notify your system programmer.

System Programmer Response: See "Problem Determination."

Problem Determination: Register 15 contains the nonzero return code passed back from the ESTAE macro. For a description of the ESTAE return code, see *z/OS MVS Programming: Authorized Assembler Services Reference ENF-IXG*.

Destination: Descriptor code is 4. Routing code is 2.

ICH517I ERROR IN RANGE TABLE.

Explanation: Either the operator entered the incorrect MLPA or LNK value, or an entry in the range table is out of order. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: If the MLPA or LNK value was incorrect, correct it and IPL again. Otherwise, notify your system programmer of the error.

Programmer Response: Ensure that the range table (ICHRRNG) was assembled and link-edited correctly. If necessary, correct the order of the entries in the range table. IPL again.

Problem Determination: The range table must contain at least one entry. The first entry must have a key of 44 binary zeroes, and the entries must appear with their keys in ascending order.

Destination: Descriptor code is 4. Routing code is 2.

ICH518I ERROR IN INITIALIZING RACF DATA SET.

Explanation: RACF unsuccessfully defined the user profile or groups to a new RACF database. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Reinitialize the new RACF databases using the IRRMIN00 utility with PARM=NEW and IPL again.

Problem Determination: The first time you IPL with RACF active, RACF generates a basic set of profiles. How these profiles are defined to each other is important. There should be one user profile (IBMUSER), and three group profiles (SYS1, SYSCATLG and VSAMDSET), the last two being subgroups of SYS1. IBMUSER must be connected to each of the three groups.

Destination: Descriptor code is 4. Routing code is 2.

**ICH519I ERROR DURING UNALLOCATION OF
RACF DATA SET.**

Explanation: There was an error during an attempt to allocate a RACF resource because RACF could not dynamically deallocate a database specified in the data set name table (ICHRDSNT) or specified in a response to the operator. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Ensure that the databases actually exist and that they reside on the DASD volume that is specified in the catalog entry of the data set. Correct the error and IPL again.

Destination: Descriptor code is 4. Routing code is 2.

**ICH520I z/OS Security Server (RACF xxxxxx) is
active.**

Explanation: RACF FMID xxxxx has been successfully initialized.

System Action: IPL continues with RACF active.

Destination: Descriptor code is 4. Routing code is 2.

**ICH521I GLOBAL ACCESS CHECKING BASE
TABLE NOT OBTAINED, NO STORAGE
AVAILABLE.**

Explanation: The attempt to obtain storage from subpool 241 for the global-profile-base-name table failed.

System Action: RACF initialization continues, but global access checking is disabled.

Operator Response: Notify the RACF security administrator and the system programmer.

Programmer Response: Check the amount of storage available for use with subpool 241 and, if necessary, increase the amount of CSA available.

Destination: Descriptor code is 4. Routing code is 2.

**ICH522I ERROR IN STARTED PROCEDURES
TABLE**

Explanation: In the started procedures table, RACF found either a generic entry that was not the last entry or a generic entry that contains '=' in both the user ID and group name fields.

System Action: RACF initialization continues, but the generic entry is ignored.

Operator Response: Notify your system programmer.

Programmer Response: Correct the started procedures table, and if necessary, IPL again.

Destination: Descriptor code is 4. Routing code is 2.

ICH523I ERROR DURING SVC TABLE UPDATE

Explanation: RACF encountered an error while trying to update the SVC table with the RACF SVC entry points. Message ICH501I follows this message.

System Action: A system dump is produced. IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Determine the cause of the error and correct it.

Destination: Descriptor code is 4. Routing code is 2.

**ICH524I INSTALLATION CLASS DESCRIPTOR
TABLE PROCESSED**

Explanation: During RACF initialization, the installation-supplied class descriptor table was located in SYS1.LINKLIB, a library concatenated to SYS1.LINKLIB, or LPA. That table is in effect for this IPL.

System Action: RACF initialization continues.

Destination: Descriptor code is 4. Routing code is 2.

**ICH525I INSTALLATION ROUTER TABLE
PROCESSED**

Explanation: During RACF initialization, the installation-supplied router table was located in SYS1.LINKLIB, a library concatenated to the SYS1.LINKLIB, or LPA. The table is in effect for this IPL.

System Action: RACF initialization continues.

Destination: Descriptor code is 4. Routing code is 2.

ICH526I RACF UNABLE TO LOCATE *modname*

Explanation: RACF encountered one of the following errors:

- RACF failed to locate the class descriptor table (ICHRRCDX) required for RACF processing. This table should be located in SYS1.LINKLIB or in a library concatenated to SYS1.LINKLIB. Processing cannot continue. Message ICH501I follows this message.
- RACF could not locate the MVS router table (ICHRFR0X.) This table should be located in SYS1.LINKLIB or in a library concatenated to SYS1.LINKLIB. Processing continues, but the user cannot invoke RACF with the RACROUTE macro instruction.

System Action: IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Correct the error and IPL again.

ICH527I • ICH531I

Destination: Descriptor code is 4. Routing code is 2.

ICH527I RACF DETECTED AN ERROR IN THE INSTALLATION ROUTER TABLE, ENTRY *entry-name*, ERROR CODE *yy*

Explanation: RACF locates the RACF router tables (ICHRFR0X and ICHRFR01) in one of the following:

- SYS1.LINKLIB
- A library concatenated to SYS1.LINKLIB
- LPA (for ICHRFR01 only).

RACF ensures that each class name satisfies certain conditions. RACF issues this message to the operator when the table contains an error.

System Action: RACF uses the first entry name and ignores additional duplicate name(s).

Operator Response: Check for errors in the specification of the system parameters MLPA and LNK. If there are errors, correct them and IPL again. If there are no errors, report the exact text of this message to your system programmer.

System Programmer Response: Ensure that no errors occurred during the assembly of the table entries, that the table was properly link-edited, and that modification subsequent to link-edit did not cause the error. Correct the error and IPL again.

Problem Determination: The error code *yy* identifies the problem as follows:

Code	Description of Error
------	----------------------

- | | |
|---|---|
| 1 | An entry in the installation-supplied portion of the router table duplicates the class name, requestor, and subsystem ID of an entry in the portion of the table supplied by IBM. |
| 2 | An entry in the installation-supplied portion of the router table has the class name specified in another installation-supplied entry. |

Destination: Descriptor code is 4. Routing code is 2.

ICH528I ERROR BUILDING PROGRAM CONTROL TABLES

Explanation: A processing error occurred as RACF attempted to build the program control tables. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: Notify the RACF security administrator and the system programmer.

Problem Determination: The SDUMP data set provides diagnostic information. Correct the error and IPL again.

Destination: Descriptor code is 4. Routing code is 2.

ICH529I RVARY ALLOCATION/DEALLOCATION FAILED

Explanation: An RVARY command was issued, and the allocation or deallocation of the RACF database failed.

User Response: Check that the data set name specified on the RVARY command is correctly spelled. If the data set name is spelled correctly, contact the system programmer.

System Programmer Response: Check that the data set specified on the RVARY command actually exists. If the data set specified on the RVARY command exists, check the DASD for problems.

Destination: Descriptor code is 4. Routing code are 2 and 11.

ICH530I I/O ERROR DURING DATASET ALLOCATION/DEALLOCATION [{PRIMARY | BACKUP } RACF DATA SET SEQUENCE *nnn*, *dsname*]

Explanation: An I/O error occurred during the allocation or deallocation of the RACF database.

System Action: The system issues message ICH502A to prompt for a new data set name.

System Programmer Response: If necessary, switch to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information on recovering from the problem, see the section on RACF database recovery in *z/OS Security Server RACF System Programmer's Guide*. Pay particular attention to the section on failures during I/O operations on the RACF database in *z/OS Security Server RACF System Programmer's Guide*.

Problem Determination: Other messages might have been issued for this problem. These messages might appear on the system console or the security console, or end users might receive them. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, which reports a return code from the RACF manager.

Destination: Descriptor code is 4. Routing code are 2 and 11.

ICH531I RACF DATASET ALLOCATION/DEALLOCATION INTERFACE IS ACTIVE.

Explanation: The facility that permits the RACF database to be allocated or deallocated automatically when the RVARY command is issued is active.

Destination: Descriptor code is 4. Routing code is 2.

ICH532I RVARV REQUEST TERMINATED DUE TO ERROR.

Explanation: An error occurred during RVARV processing.

System Action: RACF stops processing the command and issues message ICH15009I to the issuer of the RVARV command.

Operator Response: Report this message to the system programmer.

Programmer Response: IPL again and reissue the RVARV command.

Problem Determination: If this message recurs, call your IBM support center.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH533I CLASS *class-name* IS ACTIVE, BUT RACLIST FOR THE CLASS FAILED. RACLIST MACRO RETURN CODE IS *return-code*.

Explanation: At IPL, RACROUTE REQUEST=LIST processing could not be performed for the indicated class.

System Action: No in-storage profiles are created for the indicated class. RACF still protects the same resources, but system performance might be adversely affected.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Check with the RACF security administrator to see if this condition will cause a performance problem on the system. If so, re-IPL the system.

Problem Determination: See *z/OS Security Server RACROUTE Macro Reference* for the indicated return code from the REQUEST=LIST macro.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH534I CLASS *class-name* IS ACTIVE, BUT RACLIST FOR THE CLASS FAILED. RACLIST MACRO RETURN CODE IS *return-code*. REASON CODE IS *reason-code*.

Explanation: At IPL, RACROUTE REQUEST=LIST processing could not be performed for the indicated class.

System Action: No in-storage profiles are created for the indicated class. RACF still protects the same resources, but system performance might be adversely affected.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Check with the RACF security administrator to see if this condition will cause a performance problem on the system. If so, re-IPL the system.

Problem Determination: See *z/OS Security Server RACROUTE Macro Reference* for the indicated return and reason codes from the REQUEST=LIST macro.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH535I RACF DATA SET IS NOT CORRECT BLOCKSIZE. xxxxxxxx DATA SET SEQUENCE xxx, xxxxxxxx.

Explanation: The RACF data set that is identified in the message has an incorrect block size. The correct block size is 4096.

System Action: Prompts the operator to enter a new data set name.

Operator Response: Contact the system programmer.

System Programmer Response: Correct the block size of the problem data set, and notify the operator to enter the appropriate data set name.

Destination: Descriptor code is 4. Routing code is 2.

ICH537I RACF IS NOT ACTIVE. RACF IS UNABLE TO LOAD MANAGER xxxxxxxx.

Explanation: The RACF manager that is identified in the message could not be loaded from SYS1.LINKLIB. Message ICH501I follows this message.

System Action: RACF is not activated.

Operator Response: Contact the system programmer.

System Programmer Response: Check the RACF installation procedure to determine the reason the RACF manager's load module is missing from the load library. Ensure that the manager's load module is present on the load library before attempting to activate RACF.

ICH538I RACF MESSAGE TASK ABEND Sxxx.

Explanation: An ABEND occurred during RACF message subtask processing.

System Action: RACF remains active and the message subtask will attempt to restart.

Operator Response: Notify the system programmer.

Programmer Response: See "Problem Determination."

Problem Determination: See your MVS system codes

ICH539I • ICH542I

documentation for completion code Sxxx. The SDUMP data set and LOGREC data provide other diagnostic information.

Destination: Descriptor code is 4. Routing code is 2.

ICH539I UNABLE TO ESTABLISH RECOVERY ENVIRONMENT, RACF MESSAGE TASK TERMINATED.

Explanation: The RACF message subtask got a nonzero return code from an ESTAE macro instruction.

System Action: The message subtask stops. RACF remains active but RACF SRB mode services are unable to issue messages.

Operator Response: Notify the system programmer.

Programmer Response: See "Problem Determination."

Problem Determination: For a description of the ESTAE return code, see *z/OS MVS Programming: Authorized Assembler Services Reference ENF-IXG*.

Destination: Descriptor code is 4. Routing code is 2.

ICH540I RACF MESSAGE TASK TERMINATED.

Explanation: Either four recursive abends (no requests successfully processed between abends) or a total of eleven abends have occurred during RACF message subtask processing.

System Action: The message subtask stops. RACF remains active but RACF SRB mode services are unable to issue messages.

Operator Response: Notify the system programmer.

Programmer Response: See "Problem Determination."

Problem Determination: See your MVS system codes documentation for completion code Sxxx. The SDUMP data set and LOGREC data provide other diagnostic information.

Destination: Descriptor code is 4. Routing code is 2.

ICH541I RACINIT {CREATE | DELETE} FAILED. RETURN CODE IS *return-code*.

Explanation: At IPL, during RACROUTE REQUEST=LIST processing, the creation or deletion of an ACEE by way of REQUEST=VERIFY failed. The message is issued to both the operator and the security console.

System Action:

- If this occurred during creation of the ACEE, no in-storage profiles are created for any class. RACF still protects the same resources, but system performance might be adversely affected.

- If this occurred during deletion of the ACEE, in-storage profiles are created and system performance is not affected. However, storage is being wasted by the ACEE and should be deleted.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: This condition could cause a performance problem on the system. For example, on CREATE, no REQUEST=LIST processing takes place. This could cause performance degradation. If so, re-IPL the system. On DELETE, performance is not adversely affected; however, storage is being wasted by the ACEE (or ACEEs) that have not been deleted. If the problem persists, contact IBM.

Problem Determination: See *z/OS Security Server RACROUTE Macro Reference* for the indicated return and reason codes from the REQUEST=VERIFY macro.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH542I RETURN CODE FROM RACROUTE MACRO IS *return-code*.

Explanation: At IPL, during RACROUTE REQUEST=LIST processing, the REQUEST=LIST and REQUEST=VERIFY macros are invoked by RACROUTE. If one fails, RACROUTE returns its own return code as well as the return and reason codes of the called macros. For example, if the RACROUTE return code is 4, and a called REQUEST=LIST return and reason codes are 0, this means that the class is not in the router table and the REQUEST=LIST processing was not done. The message is issued to both the operator and the security console when, for example, there is an error creating an ACEE during REQUEST=LIST processing.

System Action: No in-storage profiles are created for the indicated class. RACF still protects the same resources, but system performance might be adversely affected.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: This condition could cause a performance problem on the system. For example, on CREATE, no REQUEST=LIST processing takes place. This could cause performance degradation. If so, re-IPL the system.

Problem Determination: See *z/OS Security Server RACROUTE Macro Reference* for the indicated return and reason codes from the RACROUTE macro.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH544I RACLIST DID NOT OCCUR FOR ANY OF THE RACF CLASSES CONTACT YOUR SYSTEM ADMINISTRATOR.

Explanation: During IPL, RACF initialization was not able to create an ACEE needed for RACROUTE REQUEST=LIST processing. As a result none of the RACF classes could be RACLISTed. This message is issued to both the operator and the security console.

System Action: For classes that are not part of a grouping member class pair and defined with RACLREQ=NO (REQUEST=LIST not required), normal authorization checking occurs, although system performance may be adversely affected.

For classes that are part of a grouping member class pair and defined with RACLREQ=NO (REQUEST=LIST not required), authorization checking experiences performance problems. In addition, authorization checking may be wrong, because only the profiles in the member class are considered when making decisions. The profiles in the grouping class are ignored, because they are used only when the RACLIST is successful.

For classes defined with RACLREQ=YES (REQUEST=LIST is required), ALL authorization requests for the class will result in return code 4.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: This condition could cause other components and applications to fail due to RACROUTE REQUEST=AUTH return code 4 for RACLREQ=YES classes. In addition, this condition could cause performance degradation. If either of these problems occur, re-IPL. Message ICH541I follows this message and indicates the cause of the error.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH545I WARNING: THE RACF DATA SET JUST ACTIVATED IS LOCKED. {PRIMARY | BACKUP } DATA SET SEQUENCE *nnn*, *dsname*

Explanation: During RVAR command processing, RACF detected that data set *dsname* is locked. This data set is a primary or backup data set for the sequence number indicated by *nnn*.

System Action: The RVAR ACTIVE command completes successfully. Data set *dsname* remains locked.

Operator Response: Report this message to your system programmer.

System Programmer Response: If the data set should not be locked, use the IRRUT400 utility program or the data set unload utility (IRRDBU00) to unlock the data set.

Destination: Descriptor code is 4. Routing code is 2.

ICH546I CLASS *classname* IS ACTIVE, BUT RACLIST FOR THE CLASS FAILED. DATA SPACE FAILURE RETURN CODE IS *return-code*, REASON CODE IS *reason-code*.

Explanation: At IPL, RACROUTE REQUEST=LIST processing could not be performed for the indicated class due to a problem in processing data spaces. The return and reason codes can help the IBM support center determine the cause of the problem.

System Action: For classes that are not part of a grouping member class pair, no in-storage profiles are created for the indicated class. In addition to issuing this message, the system may have taken an SVC dump. RACF still protects the same resources, but system performance may be adversely affected.

For classes that are part of a grouping member class pair, authorization checking experiences performance problems. In addition, authorization checking may be wrong, because only the profiles in the member class are considered when making decisions. The profiles in the grouping class are ignored, because they are used only when the RACLIST is successful.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Have the RACF security administrator issue SETROPTS RACLIST(*classname*). If this command fails with messages ICH14301I and ICH14058I, proceed to problem determination.

Problem Determination: Call your IBM support center. Have the message text available as well as the SVC dump if one was taken. The return code and reason code values in the message are:

Return Code	Reason Code	Explanation
04	04	ALESERV ADD function failed
	08	Data space too small
08	04	TCBTOKEN function failed
	08	DSPSERV CREATE function failed
	12	ALESERV ADD function failed

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH549I RACF DATABASE *dbname* DOES NOT RESIDE ON SHARED DASD.

Explanation: If RACF sysplex communication is desired, the RACF database must be on a shared DASD. If sysplex communication is not desired, you must turn off the data sharing bit in the data set name table (ICHRDSNT). Refer to the MVS documentation on

ICH550I • ICH554I

planning I/O configurations. This message may also be issued if RACF is installed for data sharing and a RVAR command was issued in an attempt to activate a data set that does not reside on a shared DASD. In this case, the data set will simply not be activated. Message ICH501I follows this message.

System Action: RACF enters failsoft processing.

System Programmer Response: If sysplex communication is desired, ensure the RACF database is on a shared device. Verify that the data set name table (ICHRDSNT) is accurate and re-IPL. If sysplex communication is not desired, correct the bit setting in ICHRDSNT and re-IPL.

Destination: Descriptor code is 4. Routing code is 2.

ICH550I **SYSTEM *sysname* IS IN LOCAL SYSPLEX MODE. IT CANNOT BE ENABLED FOR SYSPLEX COMMUNICATION.**

Explanation: Either the sysplex communication bit or the default mode bit in the data set name table (ICHRDSNT) is on, but the system is in local sysplex mode. In order for RACF to be enabled for sysplex communication, the system must be in non-local sysplex mode. RACF enters failsoft mode on this system. Message ICH501I follows this message.

System Action: RACF continues initialization in failsoft processing.

System Programmer Response: If sysplex communication is desired, change the system to run in non-local sysplex mode and re-IPL. Refer to the MVS documentation on planning sysplex management to determine the problem. If sysplex communication is not desired, ensure that the sysplex communication bit and the default mode bit are off in ICHRDSNT and re-IPL.

Destination: Descriptor code is 4. Routing code is 2.

ICH551I **DATA SHARING WAS REQUESTED, HOWEVER SYSTEM *sysname* IS NOT RUNNING ON THE MINIMUM MVS RELEASE LEVEL REQUIRED.**

Explanation: The indicated system is installed for data sharing but is not running on the minimum MVS release level required. Message ICH501I follows this message.

System Action: RACF continues initialization in failsoft processing.

Operator Response: Notify the system programmer.

System Programmer Response: If RACF sysplex data sharing is desired, you must upgrade the system to at least MVS 5.1.0. If RACF sysplex data sharing is not desired, you must turn off the data sharing bit in the data set name table (ICHRDSNT) and re-IPL.

Destination: Descriptor code is 4. Routing code is 2.

ICH552I **THE ATTEMPT TO BUILD THE DATA SHARING ADDRESS SPACE HAS FAILED AS INDICATED BY THE ASCRE SERVICE WITH RETURN CODE *X'retcode* AND REASON CODE *X'rsncode*.**

Explanation: The MVS service for address space creation (ASCRE) has failed with return code *retcode* and reason code *rsncode*.

System Action: RACF is initialized in read-only mode. For information about RACF sysplex data sharing modes, see *z/OS Security Server RACROUTE Macro Reference*.

System Programmer Response: Consult the MVS documentation on ASCRE return and reason codes. Attempt to fix the problem and issue the RVAR DATASHARE command. If the problem cannot be fixed, report the exact text of this message to the appropriate IBM support center.

Destination: Descriptor code is 4. Routing code is 2.

ICH553I **RACF ON SYSTEM *sysname* IS UNABLE TO JOIN GROUP IRRXCF00. IXCJOIN FAILED WITH RETURN CODE *X'retcode* AND REASON CODE *X'rsncode*.**

Explanation: RACF attempted to join the RACF sysplex data sharing group, IRRXCF00, on system *sysname*. RACF experienced failures as shown in return code *X'retcode* and reason code *X'rsncode* for the IXCJOIN service. Message ICH501I follows this message.

System Action: RACF will enter failsoft processing.

Operator Response: Notify your system programmer.

System Programmer Response: For documentation on the IXCJOIN return and reason codes, refer to the appropriate MVS documentation. If necessary, report the problem to the appropriate IBM support center.

Destination: Descriptor code is 4. Routing code is 2.

ICH554I **NUMBER OF RESIDENT DATA BLOCKS SPECIFIED IN ICHRDSNT FOR DATABASE *dbname* IS INSUFFICIENT FOR SYSPLEX COMMUNICATION. DEFAULT OF 50 FOR PRIMARY AND 10 FOR BACKUP WILL BE USED.**

Explanation: When installed for sysplex communication, RACF requires a minimum of 50 resident data blocks for the primary and a minimum of 10 resident data blocks for the backup. The number of resident data blocks specified for the primary is less than 50 for the indicated database.

System Action: RACF allocates a default of 50 resident data blocks for the primary and 10 resident

data blocks for the backup for this IPL and continues initialization.

Operator Response: Notify the system programmer.

System Programmer Response: Update the data set name table (ICHRDSNT) to specify at least 50 resident data blocks for the indicated database prior to the next IPL.

Destination: Descriptor code is 4. Routing code is 2.

ICH555I *table_name* **FOR MEMBER** *memname*
DOES NOT MATCH *table_name* **FOR**
IRRXCF00 GROUP. GROUP *table_name*
IS USED.

Explanation: There was an inconsistency between the table defined for member *memname*, and the table defined for the data sharing group, IRRXCF00. RACF uses the table defined for the data sharing group.

- If the table name is ICHRDSNT, the data set names or flag settings in the table defined for member *memname* do not match those in use by the other members of the data sharing group.
- If the table name is ICHRRNG, the contents of the range table for member *memname* do not match those in use by the other members of the data sharing group.

System Action: RACF continues initialization using the table defined for the data sharing group, IRRXCF00.

Operator Response: Notify the system programmer.

System Programmer Response: Refer to *z/OS Security Server RACF System Programmer's Guide* and correct the inconsistency in the table for member *memname* to avoid this message during the next IPL.

Destination: Descriptor code is 4. Routing code is 2.

ICH556I **RACF MANAGER INVOCATION FOR**
RVARY ENDED DUE TO ERROR.
RETURN CODE = X'nnnnnnnn'.

Explanation: This message is the result of a failure during the propagation of an RVARY request to members of the RACF data sharing group. This error was encountered during an attempt to refresh RACF control information from a newly activated master data set. The refresh may not have been completed.

The RACF manager could not complete the requested operation because of a system error or a problem with the RACF database. The return code is a RACF manager return code that is not recognized by the command processor that invoked the RACF manager.

System Action: Command processing completes, but RACF system options may not have been refreshed.

Operator Response: Report this message to your system programmer.

System Programmer Response: Determine the RACF manager problem. After the problem has been corrected, RVARY INACTIVE and RVARY ACTIVE can be issued against the master data set to ensure that RACF control information has been correctly refreshed.

Problem Determination: If there is an error in the RACF database, the RACF manager issues message ICH411I preceding this message. See this message for information on how to resolve the problem.

Note: If the user is not receiving write-to-programmer messages, message ICH411I is not received. To receive this message, issue the TSO/E command PROFILE WTPMSG MSGID and rerun the RACF command or utility.

Check the list of RACF manager return codes in "RACF Manager Return Codes" on page 307. If the return code is listed, the explanation should help you investigate the problem. If the return code is not listed or relates to a problem with RACF (as opposed to a problem you can fix in the RACF database), report the complete text of this message to your IBM support center.

For certain return codes, this message might be issued because there is a bad profile in the RACF database. To find the bad profile, enter the SEARCH command. With a bad profile in the database, this command is likely to fail also. The profile after the last one listed is probably the bad profile. Because this command might take a long time to run and might produce many lines of output, you might wish to run the command in batch mode.

Destination: Descriptor code is 4. Routing code is 2.

ICH557I **UNABLE TO ESTABLISH RECOVERY**
FOR PROPAGATED RVARY COMMAND.

Explanation: RACF attempted to process a propagated RVARY request on this member of a RACF data sharing group, but was unable to establish recovery.

System Action: RACF did not process the command on this member.

Operator Response: Report this message to your system programmer.

System Programmer Response: This might be an indication of additional system problems. Look for related messages in the system log. Correct these problems and try again. If the problem persists, call your IBM support center.

Destination: Descriptor code is 4. Routing code is 2.

ICH558I • ICH562I

ICH558I **MEMBER *memname* IS NOT AT SUFFICIENT MVS LEVEL TO EXECUTE THIS RVAR Y COMMAND.**

Explanation: All members of the RACF data sharing group must be at MVS 5.1 or above for a RVAR Y DATASHARE or RVAR Y NODATASHARE command to function. This message indicates that the member to which the command was issued was at the sufficient level but the member *memname* was not.

System Action: RACF does not process the command.

Operator Response: None.

System Programmer Response: If data sharing is desired, all the members of the RACF data sharing group must be upgraded to MVS 5.1 or above.

Destination: Descriptor code is 4. Routing code is 2.

ICH559I **MEMBER *memname* ENABLED FOR SYSPLEX COMMUNICATIONS.**

Explanation: At this point in RACF initialization, the member *memname* is enabled for sysplex communications as requested by the installation in its data set name table (ICHRDSNT). This allows the member to participate in RVAR Y and SETROPTS command propagation. Additionally, if all systems in the RACF data sharing group are at MVS 5.1 or above and the installation has a coupling facility, the member can also participate in RACF data sharing.

System Action: RACF initialization continues.

Operator Response: None.

System Programmer Response: None.

Destination: Descriptor code is 4. Routing code is 2.

ICH560I **COULD NOT CAPTURE UCB FOR RACF DATA SET. IOSCAPU FAILED WITH RETURN CODE X'*return-code*' AND REASON CODE X'*reason-code*'.**

Explanation: In MVS 5.2.0 and later environments, RACF data sets can reside on devices whose UCB is above 16MB. RACF issued the IOSCAPU macro to “capture” the UCB into a window below 16MB, and the capture request failed.

System Action: The system issues message ICH506I following this message.

If this message is received during RACF initialization, the system also issues message ICH502A following this message, which prompts the operator to enter a new data set name or 'NONE'. The system then waits for the operator's reply. Message ICH502A will not occur if this system is in data sharing mode and is not the first system in the sysplex.

If this message is received during an RVAR Y request,

message ICH502A is not issued, and the RVAR Y command retries the activation of the data set five times.

Operator Response: Notify your system programmer.

System Programmer Response: Refer to the MVS documentation for the IOSCAPU return and reason codes to determine why the UCB for the device containing the RACF data set could not be “captured” and correct the problem.

If this message was received during RACF initialization, the operator should be instructed to reply to message ICH502A with the same data set name after the problem has been corrected.

If this message was received during an RVAR Y request, the RVAR Y command should be reissued after the problem has been corrected.

ICH561I **COULD NOT UNCAPTURE UCB FOR RACF DATA SET. IOSCAPU FAILED WITH RETURN CODE X'*return-code*' AND REASON CODE X'*reason-code*'.**

Explanation: In MVS 5.2.0 and later environments, RACF data sets can reside on devices whose UCB is above 16MB. When a RACF data set is deactivated, RACF issues the IOSCAPU macro to “uncapture” a UCB that may have been “captured” into a window below 16MB when the data set was activated and the uncapture request failed.

System Action: The system issues message ICH506I following this message. Deactivation of the RACF data set continues.

Operator Response: Notify your system programmer.

System Programmer Response: Refer to the MVS documentation for the IOSCAPU return and reason codes to determine why the UCB for the device containing the RACF data set could not be “uncaptured”.

ICH562I **AN ATTEMPT TO CREATE A RACF RESOURCE MANAGER TO HANDLE ADDRESS SPACE TERMINATION HAS FAILED, AS INDICATED BY THE RESMGR SERVICE WITH RETURN CODE X'*return-code*'.**

Explanation: The MVS service for resource manager creation (RESMGR) failed with return code *return-code*.

System Action: RACF is initialized in read-only mode. For information about RACF sysplex data sharing modes, see *z/OS Security Server RACF System Programmer's Guide*.

System Programmer Response: Consult the MVS or z/OS documentation for information about RESMGR return codes and try to correct the problem.

- If you've corrected the problem, issue the RVARV DATASHARE command.
- If you cannot correct the problem, report the exact text of this message to the appropriate IBM support center.

Destination: Descriptor code is 4. Routing code is 2.

**ICH564A RACF DETECTED AN ERROR IN THE
{IBM SUPPLIED | INSTALLATION}
CLASS DESCRIPTOR TABLE, ENTRY
entry-name, ERROR CODE yy**

Explanation: RACF encountered an error for entry *entry-name*, in either the installation-defined class descriptor table, ICHRRCDX, or the class descriptor table supplied by IBM, ICHRRCDX. The class descriptor table is located in one of the following:

- SYS1.LINKLIB
- A library concatenated to SYS1.LINKLIB
- LPA (for ICHRRCDX only)

This message is followed by message ICH501I. Error code *yy* identifies the problem as follows:

Code Description of Error

- | | |
|-----------|--|
| 1 | The class name is less than 4 characters or contains embedded blanks or non-alphanumeric characters. |
| 2 | The ID field has a value of zero. |
| 3 | The POSIT mask has more than 1 bit turned on or has no bits turned on. |
| 4 | The field that defines the length of the class name (MAXLNTH or MAXLENX) has a value greater than 246. |
| 5 | The class is designated as a resource group class, but the MEMBER field does not contain a member class name. |
| 6 | The table contains more than 1024 entries. |
| 7 | Two entries have the same class names. |
| 8 | One of the following: <ul style="list-style-type: none"> • A grouped class specifies a member that does not exist in the table or is incorrect, or a member class specifies a group that does not exist in the table or is incorrect. • A pair of classes reference each other, but one or both is not a grouping class. |
| 9 | One of the reserved class names (USER, GROUP, or DATASET) appears in the class table. |
| 10 | An entry in the installation table has a class name with the same name as an entry in the table supplied by IBM. |

- | | |
|-----------|--|
| 11 | The area reserved for the pointer to the RACLSTed profiles is not zero. |
| 12 | The area reserved for the pointer to the GENLISTed profiles is not zero. |
| 13 | The length of the class descriptor table entry (as indicated in a field in the entry itself) is not the same as the actual length of the class descriptor table entry. |

System Action: IPL continues.

Operator Response: Ensure that the system parameters MLPA and LNK have been specified properly. If they are not, correct any errors and IPL again. Otherwise, notify your system programmer.

Programmer Response: Ensure that no errors occurred during the assembly of the table entries, that the table was properly link-edited, and that modifications subsequent to link-edit did not cause an error. Correct the error and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

**ICH565A RACF UNABLE TO LOCATE *modname*
IN LPA**

Explanation: RACF issues this message for two possible reasons:

- RACF searched the link-pack area and could not locate one of the routines necessary for RACF processing. Processing cannot continue. Message ICH501I follows this message.
- RACF could not locate ICHFR00 in the link-pack area. Processing continues, but the user cannot invoke RACF with the RACROUTE macro instruction.

System Action: IPL continues.

Operator Response: Ensure that the system parameters MLPA and LNK have been specified properly. If they are not, correct any errors and IPL again. Otherwise, notify your system programmer.

Programmer Response: If the system parameters MLPA and LNK have been properly specified, one of the following has happened:

- RACF has not been installed properly.
- The MLPA and LNK lists do not contain all the entries necessary to load the RACF-required modules into the link-pack area.
- There is an error in the link-edit of a required routine.

Correct the error and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH566A • ICH571A

ICH566A ERROR IN RANGE TABLE.

Explanation: Either the operator entered the incorrect MLPA or LNK value, or an entry in the range table is out of order. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: If the MLPA or LNK value was incorrect, correct it and IPL again. Otherwise, notify your system programmer of the error.

Programmer Response: Ensure that the range table (ICHRRNG) was assembled and link-edited correctly. If necessary, correct the order of the entries in the range table. IPL again.

Problem Determination: The range table must contain at least one entry. The first entry must have a key of 44 binary zeroes, and the entries must appear with their keys in ascending order.

Destination: Descriptor code is 2. Routing code is 1.

ICH567A ERROR IN INITIALIZING RACF DATA SET.

Explanation: RACF could not define the user profile or groups to a new RACF database. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Reinitialize the new RACF databases and IPL again.

Problem Determination: The first time you IPL with RACF active, RACF generates a basic set of profiles. How these profiles are defined to each other is important. There should be one user profile (IBMUSER), and three group profiles (SYS1, SYSCATLG and VSAMDSET), the last two being subgroups of SYS1. IBMUSER must be connected to each of the three groups.

Destination: Descriptor code is 2. Routing code is 1.

ICH568A ERROR DURING UNALLOCATION OF RACF DATA SET.

Explanation: An error occurred during an attempt to allocate a RACF resource because RACF could not dynamically deallocate a database specified in the data set name table (ICHRDSNT) or specified in a response to the operator. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Ensure that the databases actually exist and that they reside on the DASD volume that is specified in the catalog entry of the data set. Correct the error and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH569A ERROR DURING SVC TABLE UPDATE

Explanation: RACF encountered an error while trying to update the SVC table with the RACF SVC entry points. Message ICH501I follows this message.

System Action: A system dump is produced. IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Determine the cause of the error and correct it.

Destination: Descriptor code is 2. Routing code is 1.

ICH570A RACF UNABLE TO LOCATE *modname*

Explanation: There are two possible reasons for this message:

- RACF failed to locate the class descriptor table (ICHRCDX) required for RACF processing. This table is located in SYS1.LINKLIB or in a library concatenated to SYS1.LINKLIB.

If this is the case, processing cannot continue. Message ICH501I will follow this message.

- RACF could not locate the MVS router table (ICHRFR0X). The table is located in SYS1.LINKLIB or in a library concatenated to SYS1.LINKLIB.

If this is the case, processing continues, but the user cannot invoke RACF with the RACROUTE macro instruction.

System Action: IPL continues.

Operator Response: Notify your system programmer.

Programmer Response: Correct the error and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH571A ERROR BUILDING PROGRAM CONTROL TABLES

Explanation: A processing error occurred as RACF attempted to build the program control tables. Message ICH501I follows this message.

System Action: IPL continues.

Operator Response: Notify the RACF security administrator and the system programmer.

Problem Determination: The SDUMP data set provides diagnostic information. Correct the error and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH572A RACF IS NOT ACTIVE. RACF UNABLE TO LOAD MANAGER xxxxxxxx

Explanation: The RACF manager that is identified in the message could not be loaded from SYS1.LINKLIB. Message ICH501I follows this message.

System Action: RACF is not activated.

Operator Response: Contact the system programmer.

System Programmer Response: Check the RACF installation procedure to determine the reason the RACF manager's load module is missing from the load library. Ensure that the manager's load module is present on the load library before attempting to activate RACF.

Destination: Descriptor code is 2. Routing code is 1.

ICH573A RACF DATABASE *dbname* DOES NOT RESIDE ON SHARED DASD.

Explanation: The data set name table (ICHRDSNT) indicates that you want RACF sysplex communication, but RACF database *dbname* does not reside on the shared DASD.

This message can also be issued if RACF is installed for data sharing and the RVAR command was issued in an attempt to activate a data set that does not reside on a shared DASD. In this case, the data set is not activated. Message ICH501I follows this message.

System Action: RACF enters failsoft processing.

System Programmer Response: If you want sysplex communication, be sure the RACF database is on a shared device. Verify that the data set name table (ICHRDSNT) is accurate and IPL again. If you do not want sysplex communication, correct the bit setting in ICHRDSNT and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH574A SYSTEM *sysname* IS IN LOCAL SYSPLEX MODE. IT CANNOT BE ENABLED FOR SYSPLEX COMMUNICATION

Explanation: Either the sysplex communication bit or the default mode bit in the data set name table (ICHRDSNT) is on, but the system is in local sysplex mode. In order for RACF to be enabled for sysplex communication, the system must be in non-local sysplex mode. Message ICH501I follows this message.

System Action: RACF continues initialization in failsoft processing.

System Programmer Response: If you want sysplex communication, change the system to run in non-local sysplex mode and IPL again. Refer to the z/OS documentation on planning sysplex management to determine the problem. If you do not want sysplex

communication, turn off the sysplex communication bit and the default mode bit in ICHRDSNT and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH575A DATA SHARING WAS REQUESTED, HOWEVER SYSTEM *sysname* IS NOT RUNNING ON THE MINIMUM MVS RELEASE LEVEL REQUIRED.

Explanation: The indicated system is installed for data sharing but is not running on the minimum MVS release level required. Message ICH501I follows this message.

System Action: RACF continues initialization in failsoft processing.

Operator Response: Notify the system programmer.

System Programmer Response: If you want RACF sysplex data sharing, upgrade the system to at least MVS 5.1.0. If you do not want RACF sysplex data sharing, turn off the data sharing bit in the data set name table (ICHRDSNT) and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH576A RACF ON SYSTEM *sysname* IS UNABLE TO JOIN GROUP IRRXCF00. IXCJOIN FAILED WITH RETURN CODE *X'retcode'* AND REASON CODE *X'rsncode'*

Explanation: RACF attempted to join the RACF sysplex data sharing group, IRRXCF00, on system *sysname*. RACF experienced failures as shown in return code *X'retcode'* and reason code *X'rsncode'* for the IXCJOIN service. Message ICH501I follows this message.

System Action: RACF enters failsoft processing.

Operator Response: Notify your system programmer.

System Programmer Response: For documentation on the IXCJOIN return and reason codes, refer to the appropriate MVS documentation. If necessary, report the problem to the appropriate IBM support center.

Destination: Descriptor code is 2. Routing code is 1.

ICH577E WARNING: *segment-name* SEGMENT OF *template-type* TEMPLATE AT LEVEL *template-level* DOES NOT CONTAIN FIELD *field-name*.

Explanation: RACF initialization has determined that a critical field is missing from the templates on the RACF database. This indicates that the level of the RACF initialization code is higher than the level of the templates on the RACF database. RACF initialization continues, but functions related to this field will not be available.

If the message indicates that the LDAPPROF field of

ICH578I • ICH580I

the EIM (Enterprise Identity Mapping) segment in the USER template is missing, the following function is not available:

Enterprise Identity Mapping

If the message indicates that the ENCRYPT field of the KERB segment of the USER template is missing, then support for SETROPTS KERBLVL=1 and multiple key support for the KERB segment is unavailable, and a failure starting dynamic parse is also likely.

If the message indicates that the UNVFLG field of the BASE segment of the GROUP template is missing, then the ability to define groups with the universal group function is unavailable.

If the message indicates that the FLAG9 field of the BASE segment of the USER template type is missing, then the following functions are unavailable:

- Restricted access user ID functions
- Certificate name filter functions

If the message indicates that the KERBNAME field of the KERB segment of the USER template type is missing, then support for Network Authentication and Privacy Service is unavailable, and a failure starting dynamic parse is also likely.

If the message indicates that the ENCRYPT field of the KERB segment of the USER template is missing, then support for SETROPTS KERBLVL=1 and multiple key support for the KERB segment is unavailable, and a failure starting dynamic parse is also likely.

If the message indicates that the RACDHDR field of the BASE segment of the GENERAL template is missing, then a failure starting dynamic parse is likely and the following functions are unavailable:

- Support for hardening the cache to the RACF database as profiles in the CACHECLS class, or restoring the cache from those profiles, during the processing of an R_cacheserv callable service.
- RACF command support for User and General Resource profile PROXY segments.

Dynamic parse is required to parse segment-related keywords. It is used to add, list, alter, or delete DFP, TSO, or any other non-base segment information with the RACF commands. When dynamic parse fails to start, command processors that allow segment information will not work.

System Action: IPL continues, but certain RACF functions may not be available.

Operator Response: Notify your system programmer.

System Programmer Response: Run IRRMIN00 with PARM=UPDATE to update the templates to the correct level. Ensure that the correct RACF database has been

specified. After you run IRRMIN00, you will need to re-IPL before the template changes become effective. If you are already using the function that is not available, you should re-IPL as soon as possible after you update the templates. If you are not currently using this function, you may re-IPL at any convenient time after you perform the update. The function will remain unavailable until you re-IPL.

Destination: Descriptor code is 11. Routing codes are 1, 9 and 10.

ICH578I REQUEST FOR EIM REGISTRY FAILED. ICHEINTY RETURN CODE xxx AND REASON CODE xxx.

Explanation: An unexpected return code was received from ICHEINTY while attempting to retrieve the EIM RACF registry name.

System Action: IPL continues. EIM applications using the default registry name will not function correctly.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Determine the cause of the error, correct it, and try again. If the problem persists, contact your RACF Security Administrator.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH580I WARNING: UACC(READ) WILL BE ASSUMED FOR PROGRAMS FROM SYS1.LINKLIB PROTECTED BY PROGRAM * OR **

Explanation: The PROGRAM class profile * or ** has been specified with UACC(NONE) and dataset SYS1.LINKLIB. The operating system must have access to programs in this dataset. If any task obtains access using this profile through the UACC value, RACF will return to the caller an access value of READ. In addition, if ID(*) with ACC(NONE) is specified on the access list and is used for authorization, RACF will return to the caller an access value of READ.

System Action: Processing continues for SETROPTS. RACF will return to the caller an access value of READ for any program control access to SYS1.LINKLIB through UACC(NONE) or through ID(*) ACC(NONE).

User Response: Report this message to system administrator and system programmer. This use of UACC(NONE) or ID(*) ACC(NONE) with SYS1.LINKLIB might cause system problems.

Destination: The descriptor code is 4. The routing code is 9 and 11.

RACF Status Messages

ICH702A **ENTER PASSWORD TO {ACTIVATE | DEACTIVATE} RACF JOB=***jobname*,
USER=*userid*.

Explanation: The user has issued the RVAR command to switch RACF status. The indicated job name and user ID are those of the person who issued the RVAR command. RACF routes this message to the security console and the master console.

System Action: RACF waits for the operator to enter the password to allow the RVAR command to complete, or to enter another response (including a blank line) to cancel the command.

Operator Response: Ensure that the request has been made by an authorized person within your installation. If it has, reply with the correct password; otherwise, enter a null response to cancel the RVAR command.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

ICH703A **ENTER PASSWORD TO SWITCH RACF {DATA SETS | MODE} JOB=***jobname*,
USER=*userid*

Explanation: The RVAR command has been entered to switch RACF data sets or to change mode. The indicated job name and user ID are those of the issuer of the RVAR command. RACF routes this message to the security console and the master console.

System Action: RACF waits for the operator to enter the password to allow the RVAR command to complete, or to enter another response (including a blank line) to cancel the command.

Operator Response: Ensure that the request has been made by an authorized person within your installation. If it has, reply with the correct password; otherwise, enter a null response to cancel the command.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

RACROUTE REQUEST=AUTH Operator Messages

ICH801I '*accessor*' **ATTEMPTING** '*access-type*'
ACCESS OF ENTITY '*name*'

Explanation: A RACROUTE REQUEST=AUTH has been issued during a time when RACF processing is inactive. Because RACF is inactive, it allows access to the following:

- Resources accessed by started tasks that are marked as privileged or trusted in the RACF started procedures table (ICHRIN03)
- A user's own data sets
- Any other resources to which the operator allows access.

This message provides a record of the accesses to RACF-protected resources during the period when RACF is inactive.

The *accessor* represents a user ID, job name, or started-task name. The *access-type* represents the intended mode of system access (such as ALTER, CONTROL, UPDATE, or READ). The *name* is the name of the resource to which access was attempted, such as a data set name or a volume serial number. The *name* is one of the following:

- The name as specified on the RACROUTE macro (if SETROPTS REALDSN is in effect)
- The name as modified according to RACF naming conventions (if SETROPTS NOREALDSN is in effect).

System Action: If the accessor is a started task or a user accessing his own resource, RACF allows the access without operator intervention. If not, RACF issues message ICH802D requesting that the operator allow or deny the access.

Operator Response: If RACF does not automatically allow the access, the following message ICH802D will ask the operator to allow or deny access.

Destination: Descriptor code is 4. Routing codes are 1, 2, 9, and 11.

ICH802D **REPLY Y OR N TO THE REQUEST.**

Explanation: This message appears when RACF is inactive and a RACROUTE REQUEST=AUTH is issued on a protected resource. It follows message ICH801I which asks the operator to decide if the requestor should be allowed access to the resource.

System Action: The requesting task waits for the operator's reply. If the operator responds with N, the request is denied with, in some cases, an abend code. If the response is Y, the request is allowed, and processing continues.

Operator Response: The preceding message

ICH801I informs the operator about the resource being requested and the user ID, job name, or started-task name of the requestor. The operator uses the installation regulations to decide whether or not to allow the access.

Destination: Descriptor code is 2. Routing codes are 1, 2, 9, and 11.

RACROUTE REQUEST=DEFINE Operator Messages

ICH901I '*accessor*' **ATTEMPTING** '*access-type*'
ACCESS OF ENTITY '*name*' **IN CLASS**
'*class-name*' **[NEW NAME** '*new-name*']

Explanation: RACF issued a RACROUTE REQUEST=DEFINE during a time when RACF processing was inactive. Because RACF is inactive, it allows access to the following:

- Resources accessed by started tasks that are marked as privileged or trusted in the RACF started procedures table (ICHRIN03)
- A user's own data sets
- Any other resources to which the operator allows access.

This message informs the operator about a resource which RACF, in its inactive state, could not update in the RACF database.

The variable *accessor* represents a user ID, job name or started-task name. The variable *access-type* represents the intended mode of resource definition or update, such as DEFINE, ADDVOL, DELETE, or CHGVOL. The variable *name* is a RACF profile name, such as a data set name or a volume serial number. The variable *class-name* is one of the valid RACF class names. The variable *new-name* represents the new name of a data set being renamed.

System Action: Processing continues with RACF inactive.

Operator Response: Report this message to the system programmer and the RACF security administrator.

Programmer Response: After RACF is reactivated, determine the status of the specified resource in the RACF database. If it is not valid, use the RACF commands to update the RACF database.

Destination: Descriptor code is 4. Routing codes are 1, 2, 9, and 11.

ICH902I **WARNING:** *accessor* **SPECIFIED A 3-BYTE EXPIRATION DATE ON A RACROUTE REQUEST=DEFINE FOR A DATA SET NAME** *name*.

Explanation: A RACROUTE REQUEST=DEFINE macro was invoked and specified the EXPDT keyword, which is the address of a 3-byte expiration date. A 3-byte expiration date can only specify a date in the range 1900-1999. This warning message is issued because the z/OS SYS1.PARMLIB member, ALLOCxx, contained the 2DGT_EXPDT statement specifying POLICY(WARN).

accessor is the user ID, job name, or started-task name

that invoked the request. *name* is the tape data set name, or the discrete or generic profile name in the DATASET class that is specified on the ENTITY(X) keyword of the request.

System Action: Processing of the request continues.

User Response: The program specifying the EXPDT keyword needs to be changed to use the EXPDTX keyword. If it is your program, change it. If it is not your program, have the supplier of the program change it.

Additionally, inform your system programmer of the message.

System Programmer Response: Ensure that the program is changed before implementing POLICY(FAIL) on the 2DGT_EXPDT statement in the ALLOCxx SYS1.PARMLIB member.

Destination: Descriptor code is 4. Routing codes are 9 and 11.

ICH903I *accessor* **SPECIFIED A 3-BYTE EXPIRATION DATE ON A RACROUTE REQUEST=DEFINE FOR A DATA SET NAME** *name*.

Explanation: A RACROUTE REQUEST=DEFINE macro was invoked and specified the EXPDT keyword, which is the address of a 3-byte expiration date. A 3-byte expiration date can only specify a date in the range 1900-1999. This message is issued because the z/OS SYS1.PARMLIB member, ALLOCxx, contained the 2DGT_EXPDT statement specifying POLICY(FAIL).

accessor is the user ID, job name, or started-task name that invoked the request. *name* is the tape data set name, or the discrete or generic profile name in the DATASET class that is specified on the ENTITY(X) keyword of the request.

System Action: The RACROUTE REQUEST=DEFINE invocation fails with a SAF RC=8, RACF RC=8, RACF Reason Code = 80 (x'50').

User Response: The program specifying the EXPDT keyword needs to be changed to use the EXPDTX keyword. If it is your program, change it. If it is not your program, have the supplier of the program change it.

Additionally, inform your system programmer of the message.

System Programmer Response: Ensure that the program is changed. If the impact of the failure is large, consider reverting back to POLICY(WARN) on the 2DGT_EXPDT statement in the ALLOCxx member of SYS1.PARMLIB until the program can be changed.

Destination: Descriptor code is 4. Routing codes are 9 and 11.

Chapter 2. ICH messages for RACF commands

This section lists the command messages issued by RACF during the processing of the RACF commands. These messages are routed to the user who issued the command. See “Recovery Procedures” in *z/OS Security Server RACF System Programmer’s Guide* for procedures to recover from errors that occur during the processing of the RACF commands.

The format of the command messages is:

`ICHxxnnnt text`

where:

ICH identifies the message as a RACF message.

xx is the command processor issuing the message.

nnn is the message serial number.

t is the type code (I=information, A=action).

text is the text of the message.

The values for the **xx** field, which identifies the command processor, are:

xx	Command
00	ADDGROUP
01	ADDUSER
02	CONNECT
03	REMOVE
04	DELUSER
05	DELGROUP
06	PERMIT
08	PASSWORD
09	ADDSD and DELSD
10	RDEFINE
11	RALTER
12	RDELETE
13	RLIST
14	SETROPTS
15	RVARY
20	ALTGROUP
21	ALTUSER
22	ALTDSD
30	LISTUSER
31	SEARCH
32	LISTGRP

ADDGROUP command messages

ICH00002I NOT AUTHORIZED TO ISSUE ADDGROUP

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH00003I UNABLE TO ACCESS *group-name*

Explanation: RACF could not find the description of the indicated superior group.

System Action: Command processing stops.

ICH00004I COMMAND ENDED DUE TO ERROR

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH00005I RECOVERY UNSUCCESSFUL

Explanation: As issued, the ADDGROUP command began to update more than one profile in the RACF database. However, a system or RACF failure occurred during command processing.

System Action: To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes

could be backed out. This message follows message ICH00006I.

User Response: Report this message and the exact text of message ICH00006I to your system programmer.

Problem Determination: The RACF utility programs may be needed to correct the RACF database.

ICH00006I *group-name* NOT ADDED -or- *group-name* AND REMAINING GROUPS NOT ADDED -or- GROUP(S) NOT ADDED

Explanation: The group indicated in the message was not added. The remaining groups will be added.

ICH00007I INSUFFICIENT AUTHORITY TO SUPERIOR GROUP

Explanation: You do not have sufficient authority to issue the ADDGROUP command.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH00008I OWNER-GROUP AND SUPERIOR GROUP MUST BE THE SAME

Explanation: When the owner of a group is another group, the owning group and the superior group must be the same.

System Action: Command processing stops.

ICH00009I NOT AUTHORIZED TO INCLUDE DFP SEGMENT IN GROUP PROFILE *group-name* GROUP PROFILE WAS NOT DEFINED

Explanation: You are not authorized to add DFP segment information to the specified group profile.

System Action: Command processing stops with no update to the specified group profile.

User Response: See your RACF security administrator for authority to the DFP segment of this group profile.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

ICH00010I • ICH00011I

ICH00010I **Group *group-name* is specified multiple times on the command.**

Explanation: You are not allowed to specify the same group more than once on the command.

System Action: The duplicate group is identified. No group is added.

User Response: Reissue the command without the duplicate group name.

ICH00011I **No group is added.**

Explanation: See accompanying message ICH00010I.

System Action: Command processing ends with no group added.

User Response: Using the information in message ICH00010I, correct the syntax and reissue the command.

ADDUSER command messages

ICH01001I NOT AUTHORIZED TO SPECIFY {AUDITOR, OPERATIONS, SPECIAL}, OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the keywords shown.

System Action: The command continues with the attributes NOOPERATIONS, NOSPECIAL, or NOAUDITOR.

User Response: Report this message to your RACF security administrator.

ICH01002I NOPASSWORD OPERAND IGNORED

Explanation: You specified the NOPASSWORD operand but did not specify the OIDCARD operand. A user must have either a password or operator identification card specified.

System Action: RACF ignores the NOPASSWORD operand and assigns the user the default password.

ICH01003I NOT AUTHORIZED TO SPECIFY CLAUTH FOR {TAPEVOL, USER, DASDVOL, TERMINAL}, CLASS IGNORED

Explanation: You do not have sufficient authority to specify CLAUTH for the indicated class.

System Action: RACF ignores this class and continues with the next class or operand.

User Response: Report this message to your RACF security administrator.

ICH01004A ENTER OPERATOR IDENTIFICATION CARD

Explanation: You have specified the OIDCARD operand. This message is requesting that you enter the operator identification card for the user being defined so that the information on it can be put into the user profile.

System Action: Command processing waits for you to enter the operator identification card.

ICH01005I NOT AUTHORIZED TO ISSUE ADDUSER

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH01006I COMMAND ENDED DUE TO ERROR TERMINAL TYPE NOT SUPPORTED

Explanation: You specified the OIDCARD operand, but when the operator identification card was entered, it could not be verified because it was entered on a terminal that is not supported.

System Action: Command processing stops.

ICH01007I COMMAND ENDED DUE TO ERROR UNABLE TO PROMPT FOR OIDCARD

Explanation: You specified the OIDCARD operand, but TSO/E was unable to prompt you to enter the operator identification card.

User Response: Be sure you are executing the command in the foreground and in prompt mode.

ICH01008I COMMAND ENDED DUE TO ERROR UNABLE TO ESTABLISH ESTAE

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH01009I RECOVERY UNSUCCESSFUL

Explanation: As issued, the ADDUSER command began to update more than one profile in the RACF database. However, a system or RACF failure occurred during command processing.

System Action: To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes

ICH01010I • ICH01019I

could be backed out. This message follows message ICH01010I.

User Response: Report this message and the exact text of message ICH01010I to your system programmer.

Problem Determination: The RACF utility programs may be needed to correct the RACF database.

ICH01010I *userid* NOT ADDED -or- *userid* AND REMAINING USERS NOT ADDED -or- USER(S) NOT ADDED

Explanation: The indicated user ID was not added. The remaining user IDs will be added. This message is also issued if the SETROPTS NJEUSERID or SETROPTS UNDEFINEDUSER is used on an ADDUSER.

ICH01011I INSUFFICIENT AUTHORITY

Explanation: You do not have sufficient authority to issue the ADDUSER command.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH01012I COMMAND ENDED DUE TO ERROR PUTGET ERROR RETURN CODE IS *return-code*

Explanation: You specified the OIDCARD operand, but the TSO/E PUTGET service routine failed with the indicated return code while trying to read the operator identification card. For an explanation of the return code, see *z/OS TSO/E Programming Services*.

ICH01013I COMMAND PROCESSING TERMINATED. NO {SECLEVELS | CATEGORIES} FOUND

Explanation: RACF could not validate the name you specified on the SECLEVEL or ADDCATEGORY parameter. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined but it does not contain any members.

System Action: Command processing stops.

ICH01015I COMMAND PROCESSING COMPLETED BUT UNABLE TO UPDATE 'SYS1.BROADCAST'.

Explanation: RACF could not update the TSO/E data set SYS1.BROADCAST.

System Action: The ALTUSER command completed successfully and the user profile in the RACF database has been updated.

User Response: Report this message to your system programmer.

System Programmer Response: Check to ensure that data set SYS1.BROADCAST exists on the system and is available to RACF.

ICH01016I SIZE SPECIFIED GREATER THAN MAXSIZE, SIZE ADJUSTED TO EQUAL TO MAXSIZE

Explanation: The specified SIZE is greater than the maximum allowable size, as specified on the MAXSIZE operand.

System Action: RACF adds a user profile, but adjusts SIZE to equal the MAXSIZE operand.

User Response: To change the SIZE or MAXSIZE operands for this user profile, use the ALTUSER command.

ICH01017I ADDUSER failed. SECLABEL *seclabel-name* is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name matches the security label indicated in the message.

System Action: Command processing stops.

User Response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, define a profile with that name in the SECLABEL class. If you cannot define the profile, report the exact text of this message to your RACF security administrator.

ICH01019I User *username* is assigned an OMVS UID, but default group *grpname* does not have a GID. Processing continues.

Explanation: This is a warning message that gets issued if a user with an OMVS UID gets added and has a default group which does not have a GID.

User Response: This usage violates documented rules. Either the default group should be assigned a GID, or the UID should be removed from the user profile.

RACF Security Administrator Response: Follow documented guidelines to assure that default groups for (OMVS users with UIDs) have GIDs assigned.

CONNECT command messages

ICH02001I COMMAND ENDED DUE TO ERROR

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH02002I RECOVERY UNSUCCESSFUL

Explanation: A system or RACF failure occurred when the CONNECT command began to update more than one profile in the RACF database.

System Action: To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes could be backed out. This message follows message ICH02003I.

User Response: Report this message and the exact text of message ICH02003I to your system programmer.

Problem Determination: The RACF utility programs may be needed to correct the RACF database.

ICH02003I *userid* NOT CONNECTED -or- *userid* AND REMAINING USERS NOT CONNECTED -or- USER(S) NOT CONNECTED

Explanation: The indicated user ID and all remaining user IDs were not connected because of an error in RACF processing.

ICH02004I INSUFFICIENT AUTHORITY TO GROUP

Explanation: You do not have sufficient authority to issue the CONNECT command.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH02005I *userid* CONNECTION NOT MODIFIED

Explanation: The indicated user ID was found in the group's access list, but either no connect profile was found or an error occurred while attempting to modify the connect profile.

System Action: Command processing continues with the next user ID in the list.

ICH02006I NOT AUTHORIZED TO ISSUE CONNECT

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH02007I NOT AUTHORIZED TO SPECIFY {SPECIAL | OPERATIONS | AUDITOR}, OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the operand indicated.

System Action: RACF ignores the operand. Command processing continues with the next operand.

User Response: Report this message to your RACF security administrator.

ICH02008I AUTHORITY SPECIFIED GREATER THAN THE COMMAND USER

Explanation: You have specified a group authority on the AUTHORITY operand of the CONNECT command that is greater than your own.

System Action: Command processing stops.

User Response: Check the spelling of the group authority you specified.

ICH02009I NOT AUTHORIZED TO ALTER *userid* TO {NOSPECIAL | NOOPERATIONS | NOAUDITOR}

Explanation: You do not have sufficient authority to modify the existing group connection for the indicated user ID. You cannot specify the indicated operand.

ICH02010I • ICH02013I

System Action: RACF ignores the operand.
Command processing continues with the next operand.

User Response: Report this message to your RACF security administrator.

RACF Security Administrator Response: See *z/OS Security Server RACF Command Language Reference* for the authority required to issue the CONNECT command with the indicated operand.

ICH02010I AUTHORITY NOT ALTERED FOR *userid*

Explanation: You specified the AUTHORITY operand but an error occurred while attempting to modify the group authority field in the group profile for the indicated user ID.

System Action: Command processing continues with the next operand.

ICH02011I OWNER SPECIFIED IS NOT A RACF DEFINED USER OR GROUP

Explanation: The user ID or group name specified on the OWNER operand is not defined to RACF.

System Action: Command processing stops.

ICH02012I 'RESUME' IGNORED. *userid* NOT CURRENTLY REVOKED

Explanation: The indicated user ID is not currently revoked.

System Action: RACF ignores the specification of a future date with the RESUME operand. Command processing continues with the next operand.

ICH02013I 'REVOKE' IGNORED. *userid* IS CURRENTLY REVOKED

Explanation: REVOKE was specified with a date, but the user is already revoked.

System Action: Command processing continues with the next operand.

REMOVE command messages

ICH03002I *userid* WAS NOT CONNECTED TO GROUP

Explanation: The indicated user ID was not connected to the group so no processing could be done for the user.

System Action: Command processing continues with the next user ID in the list.

ICH03003I INSUFFICIENT AUTHORITY TO GROUP, NO USERS REMOVED

Explanation: You do not have sufficient authority to issue the REMOVE command.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH03004I COMMAND ENDED DUE TO ERROR

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH03005I *userid* CANNOT BE NEW OWNER AS USER WAS SPECIFIED TO BE REMOVED

Explanation: An attempt was made to remove the indicated user ID from a group. However, the user was also specified as the new owner of the group data set profiles and must stay connected to the group.

System Action: Those user IDs that own group data set profiles are not removed. All remaining user IDs that do not own group data set profiles are removed.

ICH03006I *userid* NOT REMOVED -or- *userid* AND REMAINING USERS NOT REMOVED -or- USER(S) NOT REMOVED

Explanation: The indicated user ID was not removed.

System Action: If this message follows ICH03004I, then no further users are removed.

ICH03007I SOME GROUP DATA SET OWNERS WERE CHANGED

Explanation: The command was not completed successfully. An error was detected while removing the user indicated in message ICH03006I.

System Action: Some of the group data sets owned by the user were modified to reflect the new owner. This was not completed.

User Response: Use the LISTDSD command to determine the status of the group data sets.

ICH03008I NOT AUTHORIZED TO ISSUE REMOVE

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH03014I *group-name* IS DEFAULT GROUP, *userid* NOT REMOVED

Explanation: A user cannot be removed from the default group. Specify the group name again or use the DELUSER command to remove the user from the default group.

ICH03021I OWNER REQUIRED FOR GROUP DATASETS, *userid* NOT REMOVED

Explanation: The indicated user ID is the owner of group data sets and cannot be removed because another owner was not specified or was invalid.

System Action: The command continues with the next user ID.

ICH03025I • ICH03026I

ICH03025I OWNER SPECIFIED NOT CONNECTED TO GROUP

Explanation: The owner specified on the command is not connected to the group.

System Action: If any user ID specified to be removed owns group data sets, message ICH03021I will be issued. The command continues with the next user ID.

ICH03026I INSTALLATION EXIT FAILED REMOVE REQUEST FOR *userid*

Explanation: The command preprocessing exit routine ICHCCX00 issued a return code of 8, indicating that RACF should fail the REMOVE request for the indicated user ID.

System Action: Processing of the REMOVE command continues with the next user ID specified.

User Response: Report this message to your system programmer.

DELUSER command messages

ICH04001I ERROR LOCATING *userid*

Explanation: The indicated user ID is not defined in the RACF database.

System Action: Command processing continues with the next user specified.

ICH04002I ERROR DELETING *userid*

Explanation: An error occurred while deleting the indicated user ID. The user profile may be in an inconsistent state.

System Action: Command processing continues with the next user specified.

ICH04004I COMMAND ENDED DUE TO ERROR

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH04006I *userid* NOT DELETED -or- *userid* AND REMAINING USERS NOT DELETED -or- USER(S) NOT DELETED

Explanation: The indicated user ID was not deleted due to an error in command processing. The remaining user IDs also may not have been deleted, depending on the type of error.

ICH04007I INSTALLATION EXIT FAILED DELETE REQUEST FOR *userid*

Explanation: The command preprocessing exit routine ICHCCX00 issued a return code of 8, indicating that RACF should fail the DELUSER request for the indicated user ID.

System Action: Processing of the DELUSER command continues with the next user ID specified.

User Response: Report this message to your system programmer.

ICH04009I *userid* CANNOT BE DELETED. DATA SET PROFILES STILL EXIST.

Explanation: The indicated user ID was not deleted from the RACF database because the data set profiles still exist for the user. All data set profiles for this user must be deleted before the user ID can be deleted.

System Action: Command processing continues with the next user.

ICH04010I NOT AUTHORIZED TO ISSUE DELUSER

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH04011I Deletion of IBMUSER not allowed.

Explanation: User IBMUSER may not be deleted from the RACF database.

System Action: RACF attempts to delete the rest of the users (if any) specified on the command line.

ICH04012I User ID *userid* cannot be deleted. One or more user ID associations exist.

Explanation: A user ID cannot be deleted while user ID associations between the user ID being deleted and other user IDs are in effect. You must delete the user ID associations before deleting the user ID.

System Action: The DELUSER command is unsuccessful; processing ends.

User Response: Delete all user ID associations between the user ID being deleted and other user IDs by using the RACLINK command with the UNDEFINE operand. If you wish to view the user ID associations between the user ID being deleted and other user IDs, issue a RACLINK command with the LIST operand.

ICH04013I User ID *userid* cannot be deleted. User ID association retrieval failed.

Explanation: The indicated user ID cannot be deleted because an error occurred while RACF attempted to retrieve user ID association information for the user ID. The status of user ID associations between the user ID being deleted and other user IDs is unknown. A user ID with user ID associations defined with other user IDs cannot be deleted. This message is accompanied by messages IRRTO04I, IRRTO05I, or IRRTO06I, which explain the error in more detail.

System Action: The DELUSER command is unsuccessful; processing ends.

User Response: Verify that the DELUSER command specified the correct user IDs to be deleted. If it did not, retry the command. If the correct user IDs were supplied, refer to the accompanying messages for more information.

ICH04014I Unable to delete certificate *certificate-name*.

Explanation: An error occurred when DELUSER attempted to delete digital certificate profile *certificate-name* in the DIGTCERT class for the user specified on the DELUSER command.

System Action: DELUSER command processing ends.

User Response: Check for additional error messages related to the problem. Issue the RACDCERT command with the LIST keyword to examine the user's certificate information. Try to issue the RACDCERT command with the DELETE keyword to delete the certificate information for this user.

ICH04015I Unable to delete ring *ring-name*.

Explanation: An error occurred when DELUSER attempted to delete ring profile *ring-name* in the DIGTRING class for the user specified on the DELUSER command.

System Action: DELUSER command processing ends.

User Response: Check for additional error messages related to the problem. Issue the RACDCERT command with the LISTRING keyword to examine the user's digital certificate key ring information. Try to issue the RACDCERT command with the DELRING keyword to delete the ring information for this user.

ICH04016I Unable to remove associated certificate mapping *mapping-profile-name*.

Explanation: An error occurred when DELUSER attempted to delete a DIGTNMAP mapping profile, *mapping-profile-name*, or remove the filter associated

with the user being deleted from this mapping profile. Profile names in the DIGTNMAP class are hashed. The actual names used to create the hash are part of the data within the profile. The message contains the hashed profile name. If the *mapping-profile-name* does not appear in the message, an error was encountered attempting to retrieve the names of the mapping profiles from the user profile.

System Action: DELUSER command processing ends for this user.

User Response: Check for additional error messages related to the problem. Issue the RACDCERT command with the LISTMAP keyword to examine the user's mapping information. Attempt to issue the RACDCERT command with the DELMAP keyword to delete the information for this user.

ICH04017I Warning: error locating certificate information for this user. Templates might be downlevel.

Explanation: An error occurred when DELUSER attempted to check for digital certificate information associated with the user being deleted. The return codes received by DELUSER indicate that the most likely cause of the problem is downlevel templates. That is, the copy of the templates currently in storage are at a lower level than the level on which you are running.

System Action: DELUSER command processing continues.

User Response: If the RACDCERT command was not used to define certificates or associate certificate mappings with this user, DELUSER continues processing and should complete successfully. Ask your system programmer to run IRRMIN00 with PARM=UPDATE to pick up the correct templates, and to schedule an IPL of this system to update the instorage templates.

If there is certificate information associated with this user, it was added from a system with the correct template level. Issue the RACF SET LIST command on all systems sharing the RACF database to determine the level of their instorage templates. Issue additional DELUSER commands from the system with the correct template level, and run the remove ID utility from that system to identify residual DIGTCERT, DIGTCRIT and DIGTNMAP profiles associated with the user deleted. Ask your system programmer to schedule an IPL of the system where the DELUSER failed to pick up the correct templates.

DELGROUP command messages

ICH05001I ERROR LOCATING *group-name*

Explanation: The specified group name is not defined in the RACF database.

System Action: Command processing continues with the next group.

ICH05002I COMMAND ENDED DUE TO ERROR

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH05004I *group-name* NOT DELETED -or- *group-name* AND REMAINING GROUPS NOT DELETED -or- GROUP(S) NOT DELETED

Explanation: The group indicated in the message and all remaining groups were not deleted.

ICH05005I NOT AUTHORIZED TO ISSUE DELGROUP

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH05006I *group-name* CANNOT BE DELETED, GROUP DATA SETS STILL DEFINED TO RACF

Explanation: The group indicated in the message was not deleted from the RACF database because there are still group data sets associated with the group. A group cannot be deleted until RACF-protection is removed from the group data sets with the DELDSD command.

System Action: Command processing continues with the next group.

ICH05007I INSTALLATION EXIT FAILED DELETE REQUEST FOR *group-name*

Explanation: The command preprocessing exit routine ICHCCX00 issued a return code of 8, indicating that RACF should fail the DELGROUP request for the indicated group name.

System Action: Processing of the DELGROUP command continues with the next group name specified.

User Response: Report this message to your system programmer.

ICH05008I WARNING *group-name* is a universal group. Run the remove ID utility to remove all users from the group.

Explanation: The group you are deleting is a universal group which does not list all members of the group within the group profile. If you do not use the REMOVE command to remove the users from the group, some user profiles could still contain a group connection for the group being deleted.

System Action: Processing of the DELGROUP command continues.

RACF Security Administrator Response: If you are executing the DELGROUP and any REMOVE commands created by the remove ID utility, then no action is required.

Otherwise, to ensure you have removed all users from the group, run the remove ID utility (IRRRID00), specifying the group name, and execute the resulting commands.

PERMIT command messages

ICH06001I *name* ALREADY AUTHORIZED TO RESOURCE - ACCESS UNCHANGED

Explanation: The indicated name (user ID or group name) in the FROM resource's access list is already on the access list of the TO resource.

System Action: Command processing continues with the next name in the FROM resource's access list.

ICH06002I *name* NOT AUTHORIZED, DELETE IGNORED

Explanation: The indicated name (user ID or group name) is not on the access list of the specified resource, and the request to delete the name from the access list is ignored.

System Action: Command processing continues with the next operand.

User Response: Check the spelling of the name indicated in the message. If the name is spelled correctly, check the spelling of the profile whose access list you want to change. For general resource profiles, check the class name as well as the profile name.

ICH06003I NOT AUTHORIZED TO ISSUE *command-name*

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH06004I *profile-name* NOT DEFINED TO RACF

Explanation: The specified profile name is not defined to RACF.

Note: If you enter the PERMIT command for a fully qualified generic profile (one whose name has no generic characters), but you do not specify the

GENERIC operand, RACF issues this message. This occurs because, without the GENERIC operand, RACF looks for a discrete profile of that name. For example, if there is a fully qualified generic profile named ABC.DATA, and you enter the following command:

```
PERMIT 'ABC.DATA' ACCESS(READ) ID(JOE)
```

RACF looks for a discrete profile named ABC.DATA and, if there is none, issues this message (ICH06004I ABC.DATA NOT DEFINED TO RACF). To identify for RACF the generic profile, specify the GENERIC operand as follows:

```
PERMIT 'ABC.DATA' ACCESS(READ) ID(JOE) GENERIC
```

Likewise, when using the FROM operand to copy an access list from a fully qualified generic profile, specify the FGNERIC operand to identify the fully qualified generic profile to RACF.

System Action: Command processing stops.

ICH06005I COMMAND ENDED DUE TO ERROR

Explanation: A RACF manager error occurred. This message is accompanied by a message explaining the error.

System Action: Command processing stops.

ICH06006I NOT AUTHORIZED TO *profile-name*

Explanation: You are not authorized to alter or copy the access list of the resource indicated by *profile-name*.

System Action: Command processing stops.

ICH06007I *name* NOT DEFINED TO RACF

Explanation: The indicated name (user ID or group name) is not defined to RACF and cannot be granted access to the resource.

System Action: Command processing continues with the next name specified on the command.

ICH06008I INSTALLATION EXIT FAILED PERMIT REQUEST FOR *profile-name*

Explanation: The command preprocessing exit routine ICHCNX00 issued a return code of 4, indicating that RACF should fail the permit request for the profile indicated in the message.

System Action: If the command attempted to modify the access list of the profile, command processing stops.

If the command attempted to copy the access list of the

profile specified on the FROM operand, only the processing associated with the ID operand is performed.

User Response: Report this message to your system programmer.

ICH06009I RESET OPTION IGNORED, CONFLICTS WITH DELETE REQUEST

Explanation: Both the DELETE and the RESET options were specified.

System Action: RACF accepts the DELETE option and ignores the RESET option.

ICH06010I {GENERIC | FGENERIC} INVALID, GENERIC COMMAND PROCESSING IS INACTIVE.

Explanation: Because the generic command processing facility is inactive, the GENERIC and FGENERIC operands are not valid.

System Action: Command processing stops.

ICH06011I RACLISTED PROFILES FOR *class-name* WILL NOT REFLECT THE UPDATE(S) UNTIL A SETROPTS REFRESH IS ISSUED

Explanation: The changes to the profiles do not become effective until the SETROPTS command is issued with the REFRESH and RACLIST operands. This message can be ignored if the following are true:

- It results from processing the RALTER command for a STARTED or DLFCLASS profile.
- The command only changed data in the STDATA or DLFDATA segments.

System Action: RACF updates the profiles in the RACF database, but does not update the in-storage copies of the profiles.

ICH06013I WHEN(*class-name*(*)) OPERAND IGNORED. INVALID WITH ACCESS OPERAND.

Explanation: A PERMIT command was issued with both the ACCESS and WHEN(*class-name*(*)) operands specified. WHEN(*class-name*(*)) is valid only when specified with the DELETE operand.

System Action: Command processing stops.

ICH06014I *userid* not authorized, DELETE ignored for WHEN(*class-name*(*resource-name*))

Explanation: The user issued the PERMIT command with the DELETE and WHEN keywords specified. The class name and resource name specified on the WHEN keyword are indicated in the message. This attempted to delete an entry from the conditional access list.

However, the entry was not found.

System Action: Command processing continues with the next DELETE request.

User Response: Check the spelling of the values specified for the ID, ACCESS, and WHEN operands, and reissue the command. To check the profile itself, enter the RLIST command with AUTHUSER specified.

ICH06015I WARNING - In class *class-name* resource *resource-name* not currently protected by RACF.

Explanation: The PERMIT command was issued with the WHEN operand specified for the indicated class. However, the indicated resource is not protected by a profile in the class.

System Action: The entry is added to the conditional access list and used by RACF when appropriate.

User Response: Ensure that the resource name specified in the WHEN operand was spelled correctly. If it was not, use the PERMIT command to delete this conditional access list entry and then create the correct entry. If the resource name is spelled correctly and you believe it should be protected by RACF, examine the profiles in the class specified in the WHEN operand to determine why the resource is not considered protected by RACF.

ICH06016I Access unchanged. *userid* already has access defined by WHEN(*class-name*(*resource-name*)).

Explanation: The user indicated in the message is already on the conditional access list with the access specified.

System Action: The conditional access list is not changed.

ICH06017I WARNING for *command-name*. Extraneous information in the FROM keyword has been ignored.

Explanation: For the PERMIT command, only one profile name (no blanks) is allowed in the FROM operand.

System Action: The first profile name (no blanks) in the FROM operand is used, and the other names are ignored.

User Response: If the access list was modified using the wrong FROM profile, delete the incorrect access list entries that were created and issue the command again.

ICH06018I • ICH06021I

ICH06018I *command-name* **failed. WHEN operand is incorrect without a value.**

Explanation: The user did not specify a keyword for the WHEN operand. Valid keywords are PROGRAM, JESINPUT, CONSOLE, APPCPORT, SYSID, or TERMINAL.

System Action: Command processing stops.

ICH06019I **WARNING: Class *class-name* is not currently active.**

Explanation: The PERMIT command was issued with the WHEN operand specified for the indicated class. However, the indicated class is not active.

System Action: The entry is added to the conditional access list, but it has no effect until the class is activated by the SETROPTS CLASSACT (*class-name*) command.

ICH06020I *command-name* **FAILED. WHEN(PROGRAM) IS INVALID FOR THIS CLASS.**

Explanation: The WHEN(PROGRAM) operand is only valid for the DATASET class.

System Action: RACF stops processing the command.

ICH06021I **PERMIT FAILED. WHEN(SYSID) IS NOT VALID FOR THIS CLASS.**

Explanation: The WHEN(SYSID) operand is only valid for the PROGRAM class.

System Action: RACF stops processing the command.

PASSWORD command messages

ICH08001I *userid* NOT DEFINED TO RACF

Explanation: The indicated user ID was not found in the RACF database.

System Action: No processing is done.

ICH08002I NEW PASSWORD CANNOT EQUAL CURRENT PASSWORD

Explanation: The new password specified must be different from the current password.

System Action: The password is not changed.

ICH08003I INTERVAL NOT IN RANGE 1-*nnn*

Explanation: The password change-interval must be greater than 0 and less than *nnn*, which is the installation-specified maximum.

System Action: The interval is not changed.

ICH08004I COMMAND ENDED DUE TO ERROR

Explanation: A RACF manager error occurred. This message is accompanied by a message explaining the error.

ICH08005I VALUE SPECIFIED IS NOT CURRENT PASSWORD

Explanation: The value specified for the current password is not correct.

System Action: The password is not changed.

ICH08006I NOT AUTHORIZED TO ISSUE PASSWORD

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH08007I NOT AUTHORIZED TO CHANGE PASSWORD/INTERVAL FOR *userid*

Explanation: You are not allowed to change the password or password interval for the user indicated in the message.

System Action: The password is not changed.

User Response: See your RACF security administrator.

ICH08008I *userid* NOT DEFINED TO USE A PASSWORD

Explanation: The indicated user ID is defined to RACF but does not require a password to enter the system.

System Action: No command processing is performed.

ICH08009I PASSWORD OPERAND IGNORED

Explanation: You specified the PASSWORD operand with the USER operand.

System Action: Only the USER operand is processed. The PASSWORD operand is ignored.

ICH08010I INTERVAL CHANGE FOR '*id*' REJECTED BY

Explanation: This is the first part of a two-part message that indicates that the installation password exit (ICHPWX01) has rejected the value you specified in the INTERVAL keyword (in the PASSWORD command).

Message ICH08012I completes this message.

System Action: Command processing stops.

User Response: See your RACF security administrator for the rules for interval values.

ICH08011I PASSWORD CHANGE FOR '*id*' REJECTED BY

Explanation: This is the first part of a two-part message indicating that the installation password exit (ICHPWX01) has rejected the character string you specified in the PASSWORD operand (on the PASSWORD command).

Message ICH08012I follows this message.

System Action: Command processing stops.

User Response: See your RACF security administrator for the rules regarding new passwords.

ICH08012I • ICH08016I

ICH08012I INSTALLATION PASSWORD EXIT

Explanation: This message completes messages ICH08010I, ICH08111I and ICH08013I.

LISTUSER command to list the KERB segment information for this user and verify that this information may be accessed. Correct any problem and ask the user to reissue the command.

ICH08013I PASSWORD AND INTERVAL CHANGES FOR *id* REJECTED BY

Explanation: This is the first of a two-part message that indicates that the installation password exit (ICHPWX01) has rejected the values you specified in both the INTERVAL and PASSWORD operands (on the PASSWORD command).

Message ICH08012I follows this message.

System Action: Command processing stops.

User Response: See your RACF security administrator for the rules for interval values and new passwords.

ICH08014I PASSWORD CHANGE REJECTED BY INSTALLATION SYNTAX RULES

Explanation: You specified a potential password that does not adhere to the syntax rules that are in effect for your installation.

System Action: Command processing stops.

User Response: See your RACF security administrator for the syntax rules for passwords.

ICH08015I NEW PASSWORD MATCHES A PREVIOUS PASSWORD FOR YOU

Explanation: You specified a password that matches a previous password. Your system restricts the use of previously used passwords.

System Action: Command processing stops.

User Response: See your RACF security administrator for password HISTORY options set by the SETROPTS command.

ICH08016I ERROR SETTING KERBEROS KEY INFORMATION

Explanation: An error occurred while attempting to generate a Kerberos key for the user changing their own password via the PASSWORD command.

System Action: All processing except for the key update is completed.

User Response: Report this message to the system programmer and provide the exact text of the command issued.

System Programmer Response: Use the RLIST command to list the KERBDFLT profile definition of the local Kerberos realm in the REALM class and verify that the local realm name (KERBNAME) is defined. Use the

ADDSD and DELDSD command messages

ICH09000I NOT AUTHORIZED TO ISSUE *command-name*

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH09001I UNABLE TO ESTABLISH ESTAE

Explanation: The command processor was unable to establish an ESTAE recovery environment.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH09002I NOT AUTHORIZED TO CREATE GROUP DATASETS FOR GROUP *group-name*

Explanation: You do not have sufficient authority to create group data sets. Processing continues with the next data set.

User Response: See your RACF security administrator or the group administrator for the group indicated in the message.

ICH09004I *profile-name* ALREADY DEFINED TO RACF

Explanation: The data set name indicated in the message was found in the RACF database.

System Action: RACF does not change the definition. Processing continues with the next data set.

ICH09005I *dsname* NOT FOUND {ON *volume* | IN CATALOG}

Explanation: If “ON *volume*” appears in the message, the specified non-VSAM data set name was not found on the indicated volume.

If “IN CATALOG” appears in the message, the specified VSAM or non-VSAM data set name was not found by a catalog search.

System Action: If the data set was not found on a particular volume, the command processor attempts to process the data set on any remaining volumes.

If the data set cannot be found in the catalog, processing continues with the next data set.

ICH09006I USER OR GROUP *name* NOT DEFINED TO RACF

Explanation: The indicated name (user ID or group name) was specified as the first-level qualifier of the data set name but could not be found on the RACF database. To protect a data set with RACF, the first-level qualifier of the data set name must be a RACF-defined user ID or group name.

System Action: Processing continues with the next data set.

ICH09007I OWNER SPECIFIED IS NOT A RACF DEFINED USER OR GROUP

Explanation: The user ID or group name specified on the OWNER operand is not defined to RACF.

System Action: Command processing stops.

ICH09008I VOLUME INFORMATION IN RACF PROFILE INCONSISTENT WITH CATALOG VOLUME INFORMATION

Explanation: In processing a request to delete RACF protection for a VSAM data set, RACF found that the volume serial number in the data set profile does not match the volume serial number in the containing catalog.

System Action: Command processing stops.

Problem Determination: Use the Access Method Services LISTCAT command and the RACF LISTDSD command to locate the inconsistency. Processing continues with the next data set.

ICH09009I • ICH09019I

ICH09009I OWNER SPECIFIED HAS INSUFFICIENT AUTHORITY TO GROUP

Explanation: For a group data set, the user ID specified on the OWNER operand does not have group authority to the group and cannot be named the owner of the group data set.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH09010I NOT AUTHORIZED TO SPECIFY NOSET

Explanation: To specify NOSET, one of the following must be true:

- Your user ID must match the first-level qualifier of the data set name.
- You must have the SPECIAL attribute.
- The data set profile is within the scope of a group in which you have the group-SPECIAL attribute.

System Action: Processing continues with the next data set.

ICH09011I NOT AUTHORIZED TO DELETE RACF PROTECTION FOR *dsname*

Explanation: You do not have sufficient access authority to delete RACF protection for the data set specified.

System Action: Processing continues with the next data set.

User Response: See your RACF security administrator.

ICH09012I *dsname* [ON *volume*] ALREADY RACF INDICATED

Explanation: While attempting to RACF-indicate the data set named in the message, the command processor found that the data set was already RACF-indicated. For a VSAM data set, the RACF indicator is in the VSAM catalog. For a non-VSAM DASD data set, the RACF indicator is in the DSCB on the volume indicated in the message. For a tape data set, the RACF indicator is in the TVTOC for the tape volume indicated in the message.

System Action: Processing continues with the next data set.

ICH09013I *dsname* [ON *volume*] IS NOT RACF INDICATED

Explanation: While attempting to remove RACF indication for the data set named in the message, the command processor found that the data set was not RACF-indicated. The RACF indicator is in the VSAM

catalog for a VSAM DASD data set, in the DSCB on the indicated volume for a non-VSAM DASD data set, or in the TVTOC for tape volume *volume*.

System Action: Processing continues with the next data set.

ICH09014I INCOMPLETE UNIT/VOLUME INFORMATION SPECIFIED

Explanation: Either unit or volume information was specified, but not both. If the data set is cataloged, do not specify unit or volume. If the data set is not cataloged, specify both unit and volume.

System Action: Command processing stops.

ICH09015I I/O ERROR ON OBTAIN ON VOLUME *volume*

Explanation: An OBTAIN issued for the data set on the volume indicated resulted in an error return code.

System Action: Command processing stops.

ICH09016I VSAM CATALOG RETURN CODE IS *rc* - REASON CODE IS IGGOCLaa - *crs*

Explanation: The return code *rc* and reason code *crs* were returned by the catalog management module IGGOCLaa as a result of a catalog error or exceptional condition. For an explanation of the return and reason codes, see the description of message IDC3009I in the system messages documentation for your system.

System Action: Processing continues with the next data set.

ICH09017I I/O ERROR PROCESSING VTOC ON VOLUME *volume*

Explanation: An I/O error occurred while reading or writing a DSCB to the volume indicated.

System Action: Command processing stops.

ICH09018I OPEN FAILED ON VOLUME *volume*

Explanation: An OPEN failed for the data set to be protected or for the VTOC data set on the volume indicated.

System Action: Command processing stops.

ICH09019I *dsname* [ON *volume*] - RACF INDICATOR INCONSISTENT WITH DATA SET PROFILE

Explanation: RACF protection was partially added or deleted for the data set indicated in the message.

System Action: The RACF indicator for the data set was processed successfully in the VSAM catalog entry, in the DSCB on DASD volume *volume*, or in the TVTOC

for tape volume *volume*, but the associated data set profile on the RACF database was not successfully processed. Processing continues with the next data set.

ICH09020I *profile-name* **NOT DEFINED TO RACF**

Explanation: The profile in the message was not found on the RACF database.

Note: If you enter the DELDSD command for a fully qualified generic profile (one whose name has no generic characters), but you do not specify the GENERIC operand, RACF issues this message. This occurs because, without the GENERIC operand, RACF looks for a discrete profile of that name. For example, if there is a fully qualified generic profile named ABC.DATA, and you enter the following command:

```
DELDSD 'ABC.DATA'
```

RACF looks for a discrete profile named ABC.DATA and, if there is none, issues this message (ICH09020I ABC.DATA NOT DEFINED TO RACF). To identify for RACF the generic profile, specify the GENERIC operand as follows:

```
DELDSD 'ABC.DATA' GENERIC
```

System Action: Processing continues with the next profile name.

ICH09021I *dsname* [ON *volume*] [AND REMAINING VOLUMES] NOT PROCESSED

Explanation: RACF processing was not successful for the indicated data set. For non-VSAM data sets, RACF processing was not successful on the volume *volume*. The phrase "AND REMAINING VOLUMES" means that all volumes sequentially after the indicated volume in the catalog entry for the data set or in the VOL list specified on the command were not processed.

ICH09022I **COMMAND PROCESSOR ENCOUNTERED SYSTEM ERROR**

Explanation: The RDJFCB function failed during the processing of the RACF indicator for a volume of a non-VSAM data set.

System Action: Command processing stops.

ICH09023I *profile-name* - **LAST VOLUME ADDED TO DATA SET PROFILE WAS** *volume*

Explanation: During processing of the ADDSD command with the NOSET operand specified, an error occurred while adding volume serials to the newly created data set profile on the RACF database. The volume *volume* was the last volume added before the error occurred.

System Action: Command processing stops.

User Response: Use the ADDVOL operand of the ALTDSD command to add the remaining volumes.

ICH09024I *dsname* **INVALID DATA SET NAME**

Explanation: The data set indicated in the message is not a valid qualified name or the first qualifier exceeded the maximum allowed length of 8 characters.

System Action: Processing continues with the next data set.

ICH09025I **NOT AUTHORIZED TO RACF PROTECT** *dsname*

Explanation: You are not authorized to RACF-protect the data set indicated in the message.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH09026I *dsname* **HAS DUPLICATE VOLUME SERIALS**

Explanation: The same volume serial was found twice in the list of volume serials for the data set indicated in the message.

System Action: RACF does not process any volumes and stops processing the command.

ICH09027I *dsname* **IN USE - TRY AGAIN LATER**

Explanation: For the VSAM data set indicated in the message, the catalog entry containing the RACF indicator cannot be modified because the data set is in use.

System Action: Processing continues with the next data set.

ICH09028I **INSTALLATION EXIT FAILED {DEFINE | DELETE} REQUEST FOR** *profile-name*

Explanation: The command preprocessing exit routine ICHCNX00 issued a return code of 4, indicating that RACF should fail the ADDSD or DELDSD request for the profile indicated in the message.

System Action: Command processing stops.

User Response: Report this message to your system programmer.

ICH09029I **ERROR ENCOUNTERED DURING VTOC PROCESSING, RETURN CODE IS** *xx*, **CVSTAT IS** *yyy*.

Explanation: The Common VTOC Access Facility (CVAF) issued a return code other than zero, indicating that a VTOC update operation was not completed successfully.

ICH09030I • ICH09038I

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: See “Problem Determination.”

Problem Determination: Return code *xx* (the contents of register 15 from a CVAF invocation) and CVSTAT value *yyy* are documented in *MVS/ESA Common VTOC Access Facility Diagnosis Reference* and *z/OS DFSMSdfp Diagnosis Reference*.

ICH09030I FILESEQ(*nnnn*) ALREADY DEFINED IN TVTOC FOR SPECIFIED VOLUME(S)

Explanation: For a tape data set, file sequence number *nnnn* is already defined in the TVTOC for the volume(s) specified. Message ICH09021I will follow this message.

System Action: Command processing continues with the next data set.

ICH09031I COMMAND PROCESSING TERMINATED. FILESEQ(*nnnn*) IS INCONSISTENT WITH CURRENT VOLUME CONTENTS

Explanation: The specified tape volumes already have data sets defined, and the file sequence number *nnnn* would fall after a multivolume data set on the first volume specified, or the second or remaining volumes are not currently empty, or the specified tape volume has been marked as a single data set volume and the file sequence number specified is greater than one.

System Action: Command processing stops.

ICH09032I UNABLE TO LOCATE TAPE VOLUME FOR DATA SET

Explanation: A specific volume for the data set was not specified. RACF attempted to locate a catalog entry for the tape data set and an entry could not be found.

System Action: Command processing stops.

User Response: Specify the correct volume for the data set.

ICH09033I TAPE DATA SET PROTECTION IS INACTIVE. TAPE IS NOT VALID

Explanation: The TAPE operand may not be specified because tape data set protection is inactive.

System Action: Command processing stops.

User Response: See your RACF security administrator for information on protecting tape data sets.

ICH09034I GENERIC INVALID, GENERIC COMMAND PROCESSING IS INACTIVE

Explanation: The GENERIC operand is not valid because the generic command processing facility is inactive.

System Action: Command processing stops.

ICH09035I COMMAND PROCESSING TERMINATED. USER NOT AUTHORIZED TO 'FROM' PROFILE *profile-name*

Explanation: The user does not have sufficient authority to the profile specified in the FROM operand.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH09036I COMMAND PROCESSING TERMINATED. 'FROM' PROFILE *profile-name* DOES NOT EXIST

Explanation: The profile name specified in the FROM operand is not an existing profile.

If the FVOLUME operand was specified, RACF could not locate a profile with the specified name and volume.

If the FVOLUME operand was not specified, one of the following is true:

- There is no profile with the specified name.
- There is more than one discrete profile with the same name protecting data sets on different volumes.

Note: For fully qualified generic names, the FGENERIC operand must be specified in order to find a matching generic profile.

System Action: Command processing stops.

ICH09037I NOT AUTHORIZED TO USE VOLUME *nnnn*

Explanation: The tape volume is already RACF-protected and the current user has insufficient authority to it.

System Action: Command processing stops.

User Response: Check the spelling of the volume on the command issued. If it is correct, see your RACF security administrator to obtain the appropriate authority.

ICH09038I COMMAND PROCESSING TERMINATED. USER SPECIFIED FOR NOTIFY NOT RACF DEFINED

Explanation: The user ID specified on the NOTIFY operand is not a RACF-defined user.

System Action: Command processing stops.

ICH09039I COMMAND PROCESSING TERMINATED. MULTIPLE TAPE DATA SETS AND MULTIPLE VOLUMES WERE SPECIFIED

Explanation: The user has specified multiple tape data sets and multiple volumes. Either multiple tape data sets or multiple volumes may be specified, but not both.

System Action: Command processing stops.

ICH09041I COMMAND PROCESSING TERMINATED. FGENERIC NOT AUTHORIZED FOR FCLASS SPECIFIED

Explanation: FGENERIC was specified, but the class indicated by FCLASS does not have generic profile checking or generic profile command processing active.

System Action: RACF stops processing the command.

ICH09042I COMMAND PROCESSING TERMINATED. NO {SECLEVELS | CATEGORIES} FOUND

Explanation: RACF could not validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System Action: RACF stops processing the command.

ICH09043I COMMAND PROCESSING TERMINATED. TAPEVOL PROFILE *profile-name* CANNOT CONTAIN A TVTOC.

Explanation: Profile *profile-name* was defined without a TVTOC. ADDSD command cannot be used.

System Action: RACF stops processing the command.

User Response: Contact your RACF security administrator.

ICH09044I NOT AUTHORIZED TO INCLUDE DFP SEGMENT IN DATASET PROFILE *dsname* DATASET PROFILE WAS NOT DEFINED

Explanation: The ADDSD command with RESOWNER operand specified was issued by a user without sufficient authority.

System Action: Command processing stops without

adding a data set profile to the RACF database.

User Response: See your RACF security administrator for authority to the DFP segment.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

ICH09045I ADDSD failed. You are not authorized to specify SECLABEL.

Explanation: The SECLABEL operand was specified on the ADDSD command, but the user does not have the SPECIAL attribute and SETROPTS SECLABELCONTROL is in effect.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH09046I DELDSD failed. There is a less specific profile *profile-name* with a different SECLABEL.

Explanation: The SETROPTS MLSTABLE option is in effect. Therefore, the execution of the particular DELDSD command could potentially change the SECLABEL of the data set, because of the existence of a less specific profile with a different SECLABEL.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH09047I ADDSD failed. There is a less specific profile *profile-name* with a different SECLABEL.

Explanation: The SETROPTS MLSTABLE option is in effect, but SETROPTS MLQUIET is not in effect. Therefore, the execution of the particular ADDSD command could potentially change the SECLABEL of the data set, because of the existence of a less specific profile with a different SECLABEL.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH09048I Your current SECLABEL *seclabel-name* has been used. FROM profile has a different SECLABEL.

Explanation: The ADDSD command was issued with FROM specified, but the FROM profile has a different SECLABEL than the profile being defined, and the SETROPTS options prevent SECLABEL changes by a

ICH09049I • ICH09059I

user without the appropriate authority. One of the following conditions is true:

- The user did not have the SPECIAL attribute, and SETROPTS SECLABELCONTROL was in effect.
- SETROPTS MLSTABLE was in effect, but SETROPTS MLQUIET was not in effect.

System Action: The command executes but the SECLABEL is not copied from the model profile. The current SECLABEL of the issuer is used.

ICH09049I ADDSD failed. SECLABEL seclabel-name is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System Action: Command processing stops.

User Response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, report the exact text of this message to your RACF security administrator.

ICH09050I RACDEF FAILED. RETURN CODE IS return-code, REASON CODE IS reason-code

Explanation: RACROUTE REQUEST=DEFINE failed for one of the following reasons:

- There is an error in an installation exit.
- An installation exit (such as ICHRD01) returned a return code of 4.
- There is an internal error.

System Action: Command processing stops.

User Response: See your RACF security administrator.

Problem Determination: See the description of return and reason codes for the REQUEST=DEFINE macro in *z/OS Security Server RACROUTE Macro Reference*. Check any related installation exit for a possible error.

ICH09051I ADDSD failed. You are not authorized to specify SECLABEL seclabel-name.

Explanation: To specify the security label indicated in the message, you must have at least READ access authority to the SECLABEL profile.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH09052I ADDSD failed. SECLABEL is required under the current RACF options.

Explanation: The SETROPTS MLACTIVE option is in effect on your system, which requires that all new profiles have a security label specified. However, the SECLABEL operand was not specified on the ADDSD command, and you have no current security label.

System Action: Command processing stops.

User Response: Specify a security label appropriate for the profile. For a description of available security labels, see your installation security procedures or your RACF security administrator.

ICH09053I Profile not deleted. This profile is the only profile providing SECLABEL protection for one or more data sets.

Explanation: You cannot delete the profile specified on the DELDSD command because it is the only remaining profile that protects one or more data sets with a security label, and the SETROPTS MLACTIVE option prevents changes to SECLABEL protection.

System Action: Command processing stops with no effect on profiles.

User Response: Check the spelling of the command you entered. If it is correct and you intend to delete this profile, rename or delete all data sets protected by the profile, then reissue the DELDSD command.

ICH09054I CATALOG NOT available. Data set, dsname, was not processed.

Explanation: The device containing the catalog has been dynamically reconfigured from the system.

System Action: Processing continues with the next data set.

User Response: Report this message to your system programmer.

System Programmer Response: Before this data set can be processed, the device containing the catalog must be dynamically re-configured back into the system.

ICH09059I MODEL parameter not valid with GENERIC profile. Parameter ignored.

Explanation: Profile names containing generic characters imply that the profile is generic. Generic profiles created with the ADDSD command cannot have a data set type of MODEL, because the MODEL and GENERIC keywords are mutually exclusive.

System Action: The MODEL keyword is ignored and the profile is added with a data set type of NON-VSAM.

RDEFINE Command Messages

ICH10004I *operand* **DOES NOT APPLY TO**
class-name **CLASS ENTITIES;**
OPERAND IGNORED

Explanation: The operand indicated in the message does not apply to the class indicated in the message.

System Action: RACF ignores the operand and continues processing with the next operand.

ICH10005I **LIST OF ENTITY NAMES SPECIFIED;**
ADDMEM OPERAND IGNORED

Explanation: The RDEFINE command was issued with a list of entity names (profile names), a class name of GLOBAL or SECDATA, and the ADDMEM operand. Only a single entity name (profile name) is allowed.

System Action: RACF ignores the ADDMEM operand. Command processing continues with the next operand.

ICH10006I **THE NEW PROFILE WILL NOT BE IN**
EFFECT UNTIL A SETROPTS REFRESH
HAS BEEN ISSUED.

Explanation: The profile class exists in common storage, but the new profile does not become effective until the SETROPTS command is issued with the REFRESH operand.

ICH10102I *profile-name* **ALREADY DEFINED TO**
CLASS *class-name*

Explanation: The indicated profile has been previously defined to RACF in the indicated class.

System Action: Command processing continues with the next profile name.

ICH10103I **NOT AUTHORIZED TO DEFINE**
profile-name

Explanation: You do not have sufficient authority to define the indicated profile to RACF.

System Action: Command processing continues with the next profile name in the list.

User Response: See your RACF security administrator.

ICH10104I **NOT AUTHORIZED TO ADD**
member-name

Explanation: You do not have sufficient authority to specify the indicated resource name on the ADDMEM operand.

System Action: Command processing continues with the next member name.

User Response: See your RACF security administrator.

ICH10105I **LEADING ZEROES ARE NOT**
ALLOWED WHEN DEFINING FOUR
CHARACTER MINIDISK. *profile-name* **IS**
NOT DEFINED.

Explanation: When specifying the profile names for minidisks that have 4-character virtual addresses, you cannot specify a zero as the first character in the virtual address. You must omit the leading zero. For example, for SMITH's 0191 minidisk, specify the following profile name:

SMITH.191

System Action: Command processing continues with the next profile name.

User Response: Change the spelling of the profile name and issue the command again.

ICH10201I **NOT AUTHORIZED TO ISSUE**
command-name

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. on adding or altering user profiles or the authority required to issue the indicated command. See *z/OS Security Server RACF Command Language Reference*.

ICH10202I **NOT AUTHORIZED TO DEFINE**
class-name **CLASS ENTITIES**

Explanation: You do not have sufficient authority to define entities (profiles) to RACF in the indicated class.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH10203I • ICH10304I

ICH10203I COMMAND PROCESSING TERMINATED. NOT AUTHORIZED TO 'FROM' PROFILE *profile-name*.

Explanation: The user does not have sufficient authority to the profile specified in the FROM operand.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH10204I COMMAND PROCESSING TERMINATED. 'FROM' PROFILE *profile-name* NOT FOUND

Explanation: The profile name specified in the FROM operand is not an existing profile.

If the FVOLUME operand was specified, RACF could not locate a profile with the specified name and volume.

If the FVOLUME operand was not specified, one of the following is true:

- There is no profile with the specified name.
- If FCLASS is DATASET, there is more than one discrete profile with the same name protecting data sets on different volumes.

Note: For fully qualified generic names with FCLASS(DATASET), the FGENERIC operand must be specified in order to find a matching generic profile.

System Action: Command processing stops.

ICH10207I COMMAND PROCESSING TERMINATED. NO {SECLEVEL | CATEGORIES} FOUND

Explanation: RACF could not validate the name you specified on the SECLEVEL or ADDCATEGORY keyword. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it contains no members.

System Action: Command processing stops.

ICH10301I *entity-name* AND REMAINING ENTITIES NOT DEFINED TO RACF

Explanation: The indicated entity name (profile name) and remaining entity names in the list were not defined to RACF because of one of the following:

- A user attempted to define (via RDEFINE) a profile containing generic characters in a class that didn't have SETROPTS GENERICs active and also specified the FROM keyword containing a profile in a class that did have SETROPTS GENERICs active.
- A RACF manager error occurred. In this case, a RACF manager error message explaining the error precedes this message.

- A system error occurred while building in-storage profiles (using RACROUTE REQUEST=LIST) for the indicated entity name.
- A system error occurred while checking (with REQUEST=FASTAUTH) the user's authority to the entities to be defined.
- A system error occurred while building in-storage profiles (using REQUEST=LIST) for the entity names specified by the ADDMEM operand, or the member class associated with the specified class is currently inactive.
- A system error occurred while checking (with REQUEST=FASTAUTH) the user's authority to the entities specified by the ADDMEM operand.
- A user with class authority (CLAUTH) but without the SPECIAL attribute attempted to define an entity in a general resource class (for example, TIMS) while the class was not active.

ICH10302I NOT AUTHORIZED TO ADD *member-name* WITH THE OPTION SPECIFIED.

Explanation: The user has attempted to add a member to a VMEVENT or VMXEVENT class profile and has specified an auditing or control option without the proper authority.

System Action: RACF stops processing the command.

User Response: See your RACF security administrator.

ICH10303I *command-name* failed. You are not authorized to specify SECLABEL.

Explanation: The command indicated in the message was issued with the SECLABEL operand. However, one of the following conditions caused the command to fail:

- The user issuing the command did not have the SPECIAL attribute, and SETROPTS SECLABELCONTROL is on.
- The SECLABEL operand was specified on the RDEFINE command, and SETROPTS MLSTABLE is on, but SETROPTS MLQUIET is not.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH10304I *command-name* failed. There is a less specific profile *profile-name* with a different SECLABEL.

Explanation: The execution of the command indicated in the message could potentially change the SECLABEL of the resource because of the existence of a less specific profile with a different SECLABEL.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH10305I Your current SECLABEL *seclabel-name* was used. FROM profile has a different SECLABEL.

Explanation: RDEFINE FROM was issued, but the FROM profile has a different SECLABEL, and the SETROPTS options preventing the SECLABEL change by a user without the appropriate authority have been turned on.

System Action: The command executes, but the SECLABEL is not copied from the model profile. The LOGON SECLABEL of the issuer is used.

ICH10306I *command-name* failed. SECLABEL *seclabel-name* is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System Action: Command processing stops.

User Response: Correct the command or define the SECLABEL.

ICH10307I SECLABEL operand ignored. It does not apply to class *class-name*.

Explanation: The SECLABEL operand was specified on the command, but SECLABEL has no meaning for the class. The operand has been ignored by the command processor.

System Action: The profile is defined, but the SECLABEL operand is ignored.

ICH10308I *command-name* failed. You are not authorized to specify SECLABEL *seclabel-name*.

Explanation: SECLABEL *seclabel-name* was specified on the command indicated in the message by a user without at least a READ authority to it.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH10309I WARNING for *command-name*. Extraneous information in the FROM keyword has been ignored.

Explanation: For the RDEFINE command, only one profile name (no blanks) is allowed in the FROM operand.

System Action: The first profile name (no blanks) in the FROM operand is used. Any characters that follow the first blank are ignored.

User Response: If the profile was created using the wrong FROM profile, delete the profile that was created and create it again.

ICH10310I *command-name* failed. User *userid* is not defined to RACF.

Explanation: The user ID indicated in the message was specified as the second qualifier in a file profile name but could not be found in the RACF database. The second qualifier in the profile name for a file must be a RACF-defined user ID.

System Action: Command processing stops.

User Response: Correct the second qualifier in the profile name and issue the command again.

ICH10311I *command-name* failed. SECLABEL is required under the current RACF options.

Explanation: The SETROPTS MLACTIVE option is in effect on your system, which requires that all new profiles have a security label specified. However, the SECLABEL operand was not specified on the indicated command, and you have no current security label.

System Action: Command processing stops.

User Response: Specify a security label appropriate for the profile. For a description of available security labels, see your installation security procedures or your RACF security administrator.

ICH10312I Profile not created. You must specify the SECLEVEL keyword when creating a SECLABEL profile.

Explanation: The user attempted to create a SECLABEL profile without specifying a security level. Each SECLABEL profile must have a security level.

System Action: The SECLABEL profile is not created.

User Response: After choosing an appropriate security level for this security label, specify it on the SECLEVEL keyword.

ICH10313I Profile cannot be defined. Profile names cannot end with '%*'.

Explanation: The user of the RDEFINE command attempted to define a profile ending with %*.

System Action: Command processing stops.

ICH10315I • ICH10317I

ICH10315I **PROFILES ARE NOT ALLOWED TO BE
ADDED TO CLASS** *class-name*.

Explanation: The user of the RDEFINE command attempted to define a profile to a class that has been defined in the class descriptor table with PROFDEF=NO specified.

System Action: RACF command processing ends.

ICH10317I **'FROM' profile** *profile-name* **is defined in
database, but is not active. SETROPTS
REFRESH may be required.**

Explanation: The profile name specified in the FROM operand is not active.

System Action: Command processing stops.

User Response: Issue the SETROPTS REFRESH command to activate the profile.

RALTER command messages

ICH11001I NOT AUTHORIZED TO SPECIFY GLOBALAUDIT FOR *profile-name*; OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the GLOBALAUDIT operand for the profile indicated in the message.

System Action: RACF ignores the operand. Command processing continues with the next operand.

User Response: See your RACF security administrator.

ICH11002I AUTHORIZED TO ISSUE ONLY GLOBALAUDIT FOR *profile-name*; REMAINING OPERANDS IGNORED

Explanation: You have specified operands in addition to GLOBALAUDIT, but you are only authorized to specify the GLOBALAUDIT operand for the indicated profile name.

System Action: RACF ignores all operands other than GLOBALAUDIT.

User Response: See your RACF security administrator.

ICH11003I NOT AUTHORIZED TO SPECIFY OWNER FOR *profile-name*; OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the OWNER operand for the indicated profile name.

System Action: RACF ignores the OWNER operand. Command processing continues with the next operand.

User Response: See your RACF security administrator.

ICH11004I *operand* DOES NOT APPLY TO *class-name* CLASS ENTITIES; OPERAND IGNORED

Explanation: The indicated operand does not apply to the indicated class.

System Action: RACF ignores the operand. Command processing continues with the next operand.

ICH11005I LIST OF ENTITY NAMES SPECIFIED; *operand* OPERAND IGNORED

Explanation: You have specified a list of entity names (profile names). Only a single entity name is allowed when either of the following is true:

- The ADDVOL or DELVOL operand is specified.

- The class name is specified as GLOBAL or SECADATA, and the ADDMEM or DELMEM operands are specified.

System Action: RACF ignores the operand. Command processing continues with the next operand.

ICH11006I NOT AUTHORIZED TO SPECIFY ADDVOL; OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the ADDVOL operand.

System Action: RACF ignores the operand. Command processing continues with the next operand.

User Response: See your RACF security administrator.

ICH11007I *entity* NAME CANNOT BE SPECIFIED IN DELVOL LIST; *profile-name* NOT DELETED

Explanation: The profile name indicated by *profile-name* matches one of the volume serial numbers specified by the DELVOL operand.

System Action: RACF ignores the request to delete the profile name. Command processing continues with the next volume serial number specified on the DELVOL operand.

ICH11008I {*seclname* | *category-name*} TO BE DELETED SHOULD BE REMOVED FROM ALL USER AND RESOURCE PROFILES

Explanation: A category or security level has been deleted from a profile in the SECADATA class. The security categories or security levels that correspond to the name(s) deleted should be deleted from all user and resource profiles or unexpected errors in RACF processing may occur.

ICH11009I RACLISTED PROFILES FOR *class-name* WILL NOT REFLECT THE UPDATE(S) UNTIL A SETROPTS REFRESH IS ISSUED

Explanation: The profile class exists in common storage, but the profile updates do not become effective until the SETROPTS command is issued with the REFRESH operand. If a RALTER command was issued that didn't change anything, updating the RACLISTED profiles via the SETROPTS REFRESH is not necessary.

ICH11102I • ICH11115I

ICH11102I *profile-name* **NOT DEFINED TO CLASS**
 class-name

Explanation: The indicated profile name has not been previously defined to RACF in the indicated class.

System Action: Command processing continues with the next profile name.

ICH11103I **NOT AUTHORIZED TO ALTER**
 profile-name

Explanation: You do not have sufficient authority to alter the indicated profile.

System Action: Command processing continues with the next profile name.

User Response: See the owner of the profile or your RACF security administrator. To display the owner of the profile, use the RLIST command.

ICH11104I *volser* **NOT IN VOLUME SET OF**
 profile-name; **VOLUME NOT DELETED**

Explanation: The indicated volume serial number (*volser*) specified on the DELVOL operand does not belong to the volume set of the indicated profile.

System Action: The volume serial number is not deleted. Command processing continues with the next operand.

ICH11105I *member-name* **ALREADY DEFINED TO**
 GROUP *profile-name*

Explanation: The resource name specified on the ADDMEM operand is already a member of the resource group being altered.

System Action: Command processing continues with the next member name.

ICH11106I *volser* **ALREADY DEFINED TO CLASS**
 TAPEVOL

Explanation: The volume serial number (*volser*) specified on the ADDVOL operand is already defined to RACF in the TAPEVOL class.

System Action: Command processing continues with the next operand.

ICH11107I *member-name* **NOT DEFINED TO**
 GROUP *profile-name*

Explanation: The resource name specified on the DELMEM operand is not a member of the resource group being altered.

System Action: Command processing continues with the next member name.

ICH11108I **NOT AUTHORIZED TO ADD**
 member-name

Explanation: The user of the RALTER command does not have sufficient authority to specify the indicated resource name on the ADDMEM operand.

System Action: Command processing continues with the next member name.

User Response: See your RACF security administrator.

ICH11111I **SINGLEDs IGNORED. VOLUME** *volser*
 CONTAINS MORE THAN ONE DATA
 SET

Explanation: The indicated volume already contains more than one entry in the TVTOC.

System Action: RACF ignores the SINGLEDs operand. Command processing continues with the next operand.

ICH11112I **TVTOC IN USE. NOTVTOC IGNORED**

Explanation: A TVTOC that protects a tape data set already exists.

System Action: RACF ignores the NOTVTOC operand. Command processing continues with the next operand.

ICH11113I **DELVOL** *volume* **PROCESSING**
 IGNORED. A TVTOC ENTRY EXISTS
 FOR A DATA SET ON THE VOLUME.

Explanation: The DELVOL operand was specified for a volume that has TVTOC entries for a tape data set(s) on the volume. The data set(s) must be deleted before the volume can be deleted.

System Action: Command processing continues with the next operand.

ICH11114I *category* **ALREADY DEFINED TO**
 profile-name

Explanation: The security category indicated in the message has already been defined in this profile.

System Action: RACF ignores the operand. Command processing continues with the next operand.

ICH11115I *category* **NOT DEFINED TO** *profile-name*

Explanation: The security category indicated in this message has not been defined to this profile.

System Action: RACF ignores the operand. Command processing continues with the next operand.

**ICH11118I COMMAND PROCESSING
TERMINATED. NO {SECLEVELS |
CATEGORIES} FOUND**

Explanation: RACF could not validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System Action: Command processing stops.

**ICH11201I NOT AUTHORIZED TO ISSUE
*command-name***

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

**ICH11301I *entity-name* AND REMAINING ENTITIES
NOT ALTERED**

Explanation: The indicated entity name (profile name) and remaining entity names in the list were not altered because of one of the following:

- A RACF-manager error occurred. In this case, the message is preceded by a RACF-manager error message explaining the error.
- A system error occurred while building in-storage profiles (using RACROUTE REQUEST=LIST) for the entity names specified by the ADDMEM operand or the member class associated with the specified class is currently inactive.
- A system error occurred while checking (with REQUEST=FASTAUTH) the user's authority to the entities specified by the ADDMEM operand.

**ICH11302I VOLUME *volser* AND REMAINING
VOLUMES NOT {ADDED | DELETED}**

Explanation: The indicated volume serial number and all remaining volumes specified on the ADDVOL or DELVOL operand were not added to or deleted from a volume set because an error occurred in the RACF manager. A RACF-manager error message precedes this message and explains the error.

System Action: Command processing stops after the other operands on the command have been processed.

**ICH11303I MEMBER *member-name* AND
REMAINING MEMBERS NOT
PROCESSED FOR ENTITY *entity-name***

Explanation: An error occurred in the RACF-manager that prevented the resource group entity name from being added to or deleted from the resource group. A RACF-manager error message precedes this message.

System Action: Other operands on the command have been processed.

**ICH11304I NOT AUTHORIZED TO ADD/DELETE
member-name WITH THE OPTION
SPECIFIED.**

Explanation: You have attempted to add a member to, or delete a member from, a profile in the VMEVENT or VMXEVENT class. However, you specified an auditing or control option that you do not have the authority to specify. The option to which you are not authorized is part of the *member-name* indicated in the message.

System Action: Command processing continues with the next member name.

User Response: See your RACF security administrator.

**ICH11306I *command-name* failed. You are not
authorized to alter a SECLABEL
profile.**

Explanation: The command indicated in the message was issued for a SECLABEL profile. However, one of the following conditions caused the command to fail:

- The user issuing the command did not have the SPECIAL attribute, and SETROPTS SECLABELCONTROL is on.
- The command indicated in the message was issued by any user while SETROPTS MLSTABLE was on, but SETROPTS MLQUIET was not.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH11307I • ICH11311I

ICH11307I *command-name* **failed. NOSECLABEL is not allowed under the current RACF options.**

Explanation: NOSECLABEL operand was specified on the command indicated in the message, and SETROPTS MLACTIVE is on.

System Action: Command processing stops.

User Response: Correct the command.

ICH11308I *command-name* **failed. SECLABEL seclabel-name is not currently defined to RACF.**

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System Action: Command processing stops.

User Response: Correct the command or define the SECLABEL.

ICH11309I **SECLABEL operand ignored. It does not apply to class *class-name*.**

Explanation: The SECLABEL operand was specified on a RACF command, but SECLABEL has no meaning for the indicated class.

System Action: The profile is defined, but the SECLABEL operand is ignored.

ICH11311I **NOSECLEVEL operation ignored. You cannot specify the NOSECLEVEL keyword for SECLABEL profiles.**

Explanation: The user attempted to delete the security level from a SECLABEL profile. Each SECLABEL profile must have a security level.

System Action: The command processor ignores the NOSECLEVEL operand. All other operands are processed.

User Response: Reconsider why you issued this command. If you wish to change the security level associated with a security label, issue the RALTER command with the new security level specified on the SECLEVEL keyword.

RDELETE command messages

ICH12001I ALL {SECLEVELS | CATEGORIES} SHOULD BE DELETED FROM USER AND RESOURCE PROFILES

Explanation: A CATEGORY or SECLEVEL profile in the SECDATA class was deleted from the RACF data set. The profile contained a member list. All security categories or security levels should be deleted from user and resource profiles, or unexpected errors in RACF processing may occur.

ICH12002I RACLISTED PROFILES FOR *class-name* WILL NOT REFLECT THE DELETION(S) UNTIL A SETROPTS REFRESH IS ISSUED.

Explanation: The profile class exists in common storage. The profile cannot be deleted until the SETROPTS command is issued with the REFRESH operand.

ICH12102I *profile-name* NOT DEFINED TO CLASS *class-name*

Explanation: The indicated profile name has not been previously defined to RACF in class *class-name*.

System Action: Command processing continues with the next profile name in the list.

ICH12103I NOT AUTHORIZED TO DELETE *profile-name*

Explanation: You do not have sufficient authority to delete the indicated profile name.

System Action: Command processing continues with the next profile name in the list.

User Response: See your RACF security administrator.

ICH12201I NOT AUTHORIZED TO ISSUE *command-name*

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the

RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH12202I COMMAND PROCESSING TERMINATED. USER DOES NOT HAVE SUFFICIENT AUTHORITY TO ALL DATA SETS IN THE TVTOC.

Explanation: The TAPEVOL profile cannot be deleted because the TVTOC in the profile contains data set(s) that have not yet passed their security retention period and the user does not have sufficient authority to delete them.

User Response: See your RACF security administrator.

ICH12301I *entity-name* AND REMAINING ENTITIES NOT DELETED

Explanation: The indicated entity name (profile name) and all remaining entity names in the list were not deleted from RACF because a RACF-manager error occurred. This message is preceded by a RACF-manager error message, which explains the error.

System Action: Command processing stops.

ICH12302I *command-name* failed. There is a less specific profile *profile-name* with a different SECLABEL.

Explanation: The execution of the command indicated in the message could potentially change the security label of the resource because of the existence of another, less specific profile with a different security label.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH12303I Profile not deleted. Deleting this profile would remove the only profile that provides SECLABEL protection for one or more resources.

Explanation: You cannot delete the profile specified on the command because it is the only remaining profile that protects one or more resources with a security label, and the SETROPTS MLACTIVE option prevents changes to SECLABEL protection.

System Action: Command processing stops with no effect on profiles.

User Response: Check the spelling of the command you entered. If it is correct and you intend to delete this profile, rename or delete all resources protected by the profile, then reissue the command.

RLIST command messages

ICH13001I NOT AUTHORIZED TO ISSUE *command-name*

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH13002I NOT AUTHORIZED TO LIST *profile-name*

Explanation: You do not have sufficient authority to list the indicated profile name.

System Action: Command processing continues with the next profile name in the list.

User Response: See your RACF security administrator.

ICH13003I *profile-name* NOT FOUND

Explanation: The indicated profile name was not found in the RACF database.

ICH13004I NOTHING TO LIST

Explanation: You specified * for profile name. Either there are no profiles in that class or you do not have sufficient authority to list any of them.

ICH13005I RESGROUP DOES NOT APPLY TO *class-name* CLASS ENTITIES; OPERAND IGNORED

Explanation: The RESGROUP operand was specified on the RLIST command and the specified class is not a "member class" (such as TERMINAL or DASDVOL) for which a resource grouping class exists.

System Action: RACF ignores the operand. Command processing continues with the next operand.

ICH13006I No profile(s) listed. NORACF specified and no other information requested.

Explanation: NORACF was specified on the RLIST command, but no segments were requested.

ICH13007I One or more requested profiles for *class-name* class are defined in the database, but are not listed. RACLIST REFRESH is required.

Explanation: The RLIST command lists database profiles. This message indicates that circumstances exist which prevent RACF from verifying your authority to list one or more requested profiles. This can occur when profiles in a RACLISTed class are added without doing RACLIST REFRESH.

System Action: Any requested profiles for the *class-name* class that the user is authorized to list are listed.

SETROPTS command messages

ICH14001I NOT AUTHORIZED TO ISSUE SETROPTS

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH14002I NOT AUTHORIZED TO SPECIFY keyword [,keyword...]; KEYWORD IGNORED.

Explanation: You do not have sufficient authority to specify the keywords indicated.

System Action: RACF ignores these keywords and continues command processing with the remaining keywords.

User Response: See your RACF security administrator.

ICH14003I I/O ERROR - *jjj*, *sss*, *ddd*, *devtyp*, *ddn*, *oper*, *xxxx*, *acc*

Explanation: A permanent I/O error occurred while processing on device *ddd*. In the message text, the error analysis information provided by the SYNADAF data management macro instruction issued by the SYNAD routine was:

jjj Job name
sss Step name
ddd Unit address of the device
devtyp Device type
ddn Data definition name
oper Operation attempted
xxxx Last seek address or block count
acc Access method

System Action: Command processing stops.

User Response: Notify your system programmer.

System Programmer Response: To recover from the problem, consider switching to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information on recovering from the problem, see the section on RACF database recovery in *z/OS Security Server RACF System Programmer's Guide*. Pay particular attention to the section on failures during I/O operations on the RACF database in *z/OS Security Server RACF System Programmer's Guide*.

Problem Determination: Other messages might have been issued for this problem. These messages might appear on the system console or the security console, or end users might receive them. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, which reports a return code from the RACF manager.

ICH14004I UNABLE TO OPEN RACF DATA SET *dsname*

Explanation: The OPEN for the indicated data set failed.

System Action: Command processing stops.

User Response: Notify your system programmer.

System Programmer Response: To recover from the problem, consider switching to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information on recovering from the problem, see the section on RACF database recovery in *z/OS Security Server RACF System Programmer's Guide*. Pay particular attention to the section on failures during I/O operations on the RACF database in *z/OS Security Server RACF System Programmer's Guide*.

Problem Determination: Other messages might have been issued for this problem. These messages might appear on the system console or the security console, or end users might receive them. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, which reports a return code from the RACF manager.

ICH14006I NOT AUTHORIZED TO CHANGE RACF OPTIONS; RACF CURRENTLY INACTIVE.

Explanation: RACF has previously been set not active by the RVARY command. RACF options cannot be changed by the SETROPTS command until the RVARY command is issued and RACF is set active again.

System Action: Command processing stops.

ICH14009I RULE_n HAS AN OVERLAPPING SPECIFICATION IN THE CONTENT RULES.

Explanation: You have tried to use the SETROPTS command to define a syntax rule for use in your installation. The position values for the content keywords overlap. The following example illustrates overlapping position values:

```
SETROPTS PASSWORD (RULE1(LENGTH(8) -
ALPHA(1:5) NUMERIC(4:8)))
```

The overlap occurs for positions 4 and 5 in the content keywords ALPHA and NUMERIC. There are several ways to correct the error, depending on your intention for the rule. For example, ...ALPHA(1:3) NUMERIC(4:8) ... is correct.

System Action: RACF ignores this rule and other rules specified by RULE_n but processes other PASSWORD options and other keywords specified on the SETROPTS command.

ICH14010I * WARNING, THIS OPTION IS INACTIVE, IT REQUIRES THE 'INITSTATS' OPTION.

Explanation: RACF requires that the INITSTATS option be in effect when you specify the LIST operand on the SETROPTS command with any of the following options: INACTIVE, REVOKE, HISTORY, or WARNING.

System Action: Command processing stops.

ICH14011I GLOBAL ACCESS CHECKING BASE TABLE IS ABSENT, NO GLOBAL ACCESS CHECKING CAN BE DONE.

Explanation: During RACF Master Scheduler Initialization processing, an error prevented construction of the global access checking base table.

System Action: Global access checking is disabled, but the GLOBAL options are set in the RACF CVT and in the RACF database ICB.

ICH14013I REFRESH IGNORED. NO RELATED KEYWORDS SPECIFIED.

Explanation: When the REFRESH operand is specified, the GLOBAL, GENERIC, GENLIST, RACLIST, or WHEN operand must also be specified to indicate what is to be refreshed.

System Action: RACF continues command processing with the other operands specified.

ICH14014I GLOBAL ACCESS CHECKING BASE TABLE IS ABSENT, REFRESH CANNOT BE DONE.

Explanation: During RACF initialization processing, an error prevented construction of the global access checking base table. You cannot perform a global access checking refresh or generic profile checking refresh.

System Action: Command processing continues with the other operands. If the system is enabled for sysplex communication, the command is propagated to other systems in the sysplex. If this condition is detected on another member of the sysplex, this message is issued on that other member's master console as a WTO.

ICH14015I NOT AUTHORIZED TO REFRESH {GLOBAL | GENERIC} CLASS *class-name*

Explanation: You do not have sufficient authority to refresh the given class.

System Action: RACF ignores this class. Command processing continues with the next operand.

User Response: See your RACF security administrator.

ICH14016I CANNOT REFRESH *class-name*, {GLOBAL | GENERIC} ACCESS CHECKING INACTIVE

Explanation: Because global access checking or generic access checking is inactive for the given class, no refresh can be done.

System Action: RACF ignores this class. Command processing continues with the next operand.

ICH14017I ERROR ENCOUNTERED DURING GROUP AUTHORITY PROCESSING; COMMAND PROCESSING TERMINATED

Explanation: A RACF manager error occurred during the processing required to determine whether the command issuer has group authority.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH14018I WARNING: TAPEDSN OPTION ACTIVE, TAPEVOL CLASS IS NOT ACTIVE

Explanation: To protect tape data sets, if your installation does not have a tape management system, RACF requires the TAPEVOL class to be active.

User Response: Use the SETROPTS command with

ICH14019I • ICH14030I

CLASSACT(TAPEVOL) specified to activate the TAPEVOL class.

ICH14019I 'RVARYPW' IGNORED. ERROR ENCOUNTERED DURING PASSWORD ENCODING.

Explanation: RACF uses an installation-defined password to approve a user's issuance of the RVARY command. The password is specified in the RVARYPW operand of the SETROPTS command. If RACF is unable to encode the password at the time the SETROPTS command is issued, you receive this message.

System Action: RACF ignores the operand and processing continues with the next operand.

User Response: Report this message to your system programmer.

ICH14020I 'WHEN/NOWHEN' OPTION IGNORED. ENVIRONMENT DOES NOT SUPPORT *class-name* CLASS

Explanation: Because it does not support the indicated class, RACF cannot implement the WHEN or NOWHEN option in this system environment.

System Action: RACF ignores the option.

ICH14021I ERROR REFRESHING *program* ACCESS TABLE. COMMAND PROCESSING TERMINATED

Explanation: An error occurred when RACF attempted to refresh the *program* access table.

System Action: Command processing stops.

ICH14023I ERROR ENCOUNTERED DURING RACLIST, NORACLIST, OR RACLIST REFRESH PROCESSING. SYSTEM STORAGE MAY NOT HAVE BEEN RECOVERED.

Explanation: An error occurred during RACLIST, NORACLIST, or RACLIST REFRESH processing, which may have caused storage loss.

ICH14024I SECDATA SECLEVEL PROFILE NOT FOUND ON RACF DATASET. COMMAND PROCESSING TERMINATED.

Explanation: No profile named SECLEVEL is defined in class SECDATA.

ICH14025I ERROR ENCOUNTERED DURING SECLEVEL PROCESSING. COMMAND PROCESSING TERMINATED.

Explanation: An error occurred when RACF attempted to process the SECLEVEL operand.

System Action: Command processing stops.

ICH14026I NOT PROCESSED FOR *class-name*, RACLIST AND GENLIST CANNOT BOTH BE ACTIVE.

Explanation: You cannot specify both RACLIST and GENLIST for the same general resource class.

User Response: Reissue the command, specifying either RACLIST or GENLIST.

ICH14027I {RACLIST | GENLIST} OF CLASS *class-name* NOT ALLOWED BY THE CLASS DESCRIPTOR TABLE. OPERAND IGNORED.

Explanation: The definition in the class descriptor table does not allow this class to be RACLISTed or GENLISTed.

System Action: RACF ignores the option.

ICH14028I CLASS *class-name* ALREADY GENLISTED. OPERAND IGNORED.

Explanation: A class can be GENLISTed only once. The class specified has already been GENLISTed using the SETROPTS command and cannot be GENLISTed again.

System Action: RACF ignores the option.

ICH14030I NOGENLIST of class *class-name* ignored. GENLIST has not been done yet.

Explanation: SETROPTS NOGENLIST is valid only for classes for which SETROPTS GENLIST has been successful.

System Action: None of the classes specified on the NOGENLIST operand was affected.

User Response: If you do not want profiles kept in storage for this class, do nothing. If you have specified more than one class on the NOGENLIST operand, none of the classes is affected by the command. Issue the SETROPTS command again, omitting the class indicated in the message from the NOGENLIST operand.

ICH14031I *request of class class-name failed.*

Explanation: The SETROPTS command was issued with one of the following specified:

- RACLIST
- RACLIST REFRESH
- NORACLIST
- NOGENLIST
- NOGENERIC

The request did not complete successfully.

Note: This message appears in uppercase when issued to the operator console.

System Action: The class indicated in the message was not affected by the SETROPTS command.

Problem Determination: The message following this message describes why the SETROPTS command failed.

ICH14032I *No in-storage profiles were found for class class-name.*

Explanation: The SETROPTS command was issued with one of the following specified:

- NOGENLIST
- NOGENERIC

The request did not complete successfully.

System Action: The class indicated in the message was not affected by the SETROPTS command.

User Response: Check that the *class-name* specified in the SETROPTS command is the class you want. If it is, the class does not have the necessary profiles.

ICH14033I *Return code from RACLIST macro is return-code.*

Explanation: The SETROPTS command processor encountered an error related to the RACROUTE REQUEST=LIST macro.

Note: This message appears in uppercase when issued to the operator console.

System Action: The class indicated in message ICH14031I was not affected by the SETROPTS command. If the system is enabled for sysplex communication and the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues.

User Response: If the message indicates a return code other than zero, issue the SETROPTS command again. If the problem persists, see your system programmer.

If the message indicates a return code of zero, and

message ICH14031I (which can appear with this message) indicates a REQUEST=LIST failure for an installation-defined class, ensure that the installation-defined class is defined in both the class descriptor table (CDT) and the RACF router table.

System Programmer Response: See “Problem Determination.”

Problem Determination: If the return code reported in this message is not zero, see the description of return codes for the REQUEST=LIST macro in *z/OS Security Server RACROUTE Macro Reference*.

ICH14034I *Reason code from RACLIST macro is reason-code.*

Explanation: The SETROPTS command processor issued the RACROUTE REQUEST=LIST macro, but received the return code reported in message ICH14033I. This message reports a related reason code.

Note: This message appears in uppercase when issued to the operator console.

System Action: The class indicated in message ICH14031I was not affected by the SETROPTS command. If the system is enabled for sysplex communication and the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues.

User Response: Issue the SETROPTS command again. If the problem persists, see your system programmer.

System Programmer Response: See “Problem Determination.”

Problem Determination: The reason code indicated in this message is related to the return code indicated in message ICH14033I. For a description of return and reason codes for the REQUEST=LIST macro, see *z/OS Security Server RACROUTE Macro Reference*.

ICH14035I *RACINIT {CREATE | DELETE} failed, return code return-code.*

Explanation: If the message indicates CREATE, then SETROPTS RACLIST processing could not create an ACEE. If the message indicates DELETE, then SETROPTS RACLIST processing could not delete an ACEE.

Note: This message appears in uppercase when issued to the operator console.

System Action: If the system is not enabled for sysplex communication, command processing stops and no classes are affected. If the system is enabled for

ICH14036I • ICH14043I

sysplex communication and the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues.

User Response: Issue the SETROPTS command again. If the problem persists, report the exact text of this message to your system programmer.

System Programmer Response: To correct the problem, re-IPL the system. If the problem persists, see "Problem Determination".

Problem Determination: For a description of the RACROUTE REQUEST=LIST return codes, see *z/OS Security Server RACROUTE Macro Reference*. Report the exact text of this message, with the exact wording of the SETROPTS command you entered, to your IBM support center.

ICH14036I Unable to {ENQ | DEQ} the class descriptor table.

Explanation: If ENQ is specified in the message, SETROPTS RACLIST (or GENLIST) processing could not obtain an exclusive lock on the class descriptor table. If DEQ is specified in the message, SETROPTS RACLIST (or GENLIST) processing could not release its lock on the class descriptor table.

System Action: Command processing stops and no classes are affected.

User Response: Issue the SETROPTS command again. If the problem persists, see your system programmer.

System Programmer Response: To correct the problem, re-IPL the system. If the problem persists, see "Problem Determination."

Problem Determination: Report the exact text of this message, with the exact wording of the SETROPTS command you entered, to your IBM support center.

ICH14037I WARNING! The MLS option is active, but the SECLABEL class is inactive.

Explanation: The SETROPTS MLS command was issued, but the SECLABEL class is not active.

System Action: There is no effect on system operation.

User Response: To put the MLS option into effect, activate the SECLABEL class.

ICH14038I WARNING! The MACTIVE option is active, but the SECLABEL class is inactive.

Explanation: The SETROPTS MACTIVE command was issued, but the SECLABEL class is not active.

System Action: There is no effect on system operation.

User Response: To put the MACTIVE option into effect, activate the SECLABEL class.

ICH14040I WARNING! You must RACLIST class *class-name* before authorization checking can occur.

Explanation: This message is issued when a class is activated by way of the SETROPTS CLASSACT(*class*) command, and the RACF class descriptor table indicates that this class must be RACLISTed before checking can occur.

System Action: RACF does not perform authorization checking (or auditing based on profiles) for the class until the indicated class has been RACLISTed.

User Response: Issue the SETROPTS RACLIST command for the class.

ICH14041I action of class *class-name* ignored. The class is not active yet.

Explanation: The SETROPTS command was issued with the RACLIST or RACLIST REFRESH operands specified. However, class *class-name* is not active.

System Action: SETROPTS RACLIST processing is not done for the class.

User Response: Activate the class and issue the SETROPTS RACLIST command.

ICH14042I action of class *class-name* ignored. The class has been marked for de-activation.

Explanation: The SETROPTS command was issued with the NOCLASSACT and RACLIST operands specified and did not complete successfully.

System Action: Class *class-name* was not affected by the SETROPTS command.

User Response: You cannot specify both the NOCLASSACT operand and the RACLIST operand for the same class. Correct the command and try again.

ICH14043I Invalid character *character* specified in the userid for *operand*. Operand ignored.

Explanation: The user ID specified on the JES(NJEUSERID) or JES(UNDEFINEDUSER) operand contained an incorrect character.

System Action: RACF ignores operand *operand*.

User Response: Change the user ID specified in the command and try again.

ICH14044I **Userid** *userid* **specified for operand already exists. Please try another userid.**

Explanation: The user ID specified on the JES(NJEUSERID) or JES(UNDEFINEDUSER) operand is already a RACF-defined user.

System Action: RACF ignores operand *operand*.

User Response: Change the user ID specified in the command and try again.

ICH14045I **RACXTRT macro for operand failed.**

Explanation: While processing the SETROPTS command, RACF issued the RACROUTE REQUEST=EXTRACT macro, and an error occurred.

System Action: Command processing stops.

User Response: Report the exact text of this message, and of message ICH14046I, to your system programmer.

System Programmer Response: See "Problem Determination".

Problem Determination: See message ICH14046I, which is issued with this message, for the return and reason codes for the REQUEST=EXTRACT macro. For a description of these return and reason codes, see *z/OS Security Server RACROUTE Macro Reference*. You should also consider checking any related installation exit for a possible error.

ICH14046I **Return code is** *return-code*, **reason code is** *reason-code*.

Explanation: This message follows message ICH14045I, and includes additional problem determination information for the error that caused message ICH14045I.

System Action: See message ICH14045I.

User Response: See message ICH14045I.

ICH14047I **Return code from RACROUTE macro is** *return-code*.

Explanation: This message follows message ICH14045I and includes additional problem determination information for the error that caused message ICH14045I. Various RACF macros are invoked by RACROUTE. If either the RACROUTE interface or the called macro fails, the RACROUTE macro returns its own return code as well as the return and reason codes of the called macro. For example, if the RACROUTE return code is 4, and the RACROUTE REQUEST=LIST return and reason codes are 0, this means that the class is not in the router table and the REQUEST=LIST processing was not done.

Note: This message appears in uppercase when issued to the operator console.

System Action: See message ICH14045I.

User Response: See message ICH14045I.

ICH14048I **Security level name** *security-level-name* **is not defined to RACF.**

Explanation: An incorrect security level name was entered on a SETROPTS ERASE-ON-SCRATCH BY SECLEVEL or SETROPTS SECLEVELAUDIT option.

System Action: The system prompts the user to reenter the command.

User Response: Check the spelling of the value specified for the security-level name and reenter the command.

ICH14049I **The PRIMARY sub-operand was ignored. value is not a valid language code.**

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM.

System Action: The installation default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Issue the SETROPTS command again with a valid language code specified.

ICH14050I **The PRIMARY sub-operand was ignored. The MVS message service is not active.**

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained because the MVS message service is not active.

System Action: The installation default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Issue the SETROPTS command again with a valid language code specified.

ICH14051I **The PRIMARY sub-operand was ignored. The specified language is not active.**

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained from the MVS message service.

System Action: The installation default for the

ICH14052I • ICH14058I

PRIMARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Issue the SETROPTS command again with a valid language code or language name specified.

ICH14052I **The SECONDARY sub-operand was ignored. value is not a valid language code.**

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM.

System Action: The installation default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Issue the SETROPTS command again with a valid language code specified.

ICH14053I **The SECONDARY sub-operand was ignored. The MVS message service is not active.**

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained because the MVS message service is not active.

System Action: The installation default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Issue the SETROPTS command again with a valid language code specified.

ICH14054I **The SECONDARY sub-operand was ignored. The specified language is not active.**

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained from the MVS message service.

System Action: The installation default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Issue the SETROPTS command again with a valid language code or language name specified.

ICH14055I **The PRIMARY sub-operand was ignored. QRYLANG failed with return code xxxx and reason code yyyy.**

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyyy.

System Action: The system-wide default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Report the complete text of this message to your system programmer.

System Programmer Response: See *z/OS MVS Programming: Authorized Assembler Services Reference LLA-SDU* for a description of return codes and reason codes for the QRYLANG macro.

ICH14056I **The SECONDARY sub-operand was ignored. QRYLANG failed with return code xxxx and reason code yyyy.**

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyyy.

System Action: The system-wide default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User Response: Report the complete text of this message to your system programmer.

System Programmer Response: See *z/OS MVS Programming: Authorized Assembler Services Reference LLA-SDU* for a description of return codes and reason codes for the QRYLANG macro.

ICH14058I **Command of class classname encountered a data space problem. Return code is return-code, reason code is reason-code.**

Explanation: The SETROPTS command processor encountered a problem creating a data space, deleting a data space, or moving data into a data space. The request can be one of the following:

- RACLIST
- RACLIST REFRESH

- NORACLIST

Note: This message appears in uppercase when issued to the operator console.

System Action: If this message is preceded by message ICH14031I, data space processing is the reason the command failed. If not, the command completed in spite of the data space problems. The return and reason codes can help the IBM support center determine the cause of the problem. In addition to issuing this message, the system may also have taken an SVC dump. If the system is enabled for sysplex communication and the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, command processing stops on all systems. Otherwise, processing continues.

User Response: If the SETROPTS command failed, re-issue it. If the problem recurs, report the exact text of this message to your system programmer.

System Programmer Response: Perform problem determination.

Problem Determination: Report the issuance of this message plus the exact wording of the SETROPTS command you entered to your IBM support center. Have the return and reason codes, as well as the SVC dump if one was taken, available.

Return Code	Reason Code	Explanation
04	04	ALESERV ADD function failed
	08	Data space too small
08	04	TCBTOKEN function failed
	08	DSPSERV CREATE function failed
	12	ALESERV ADD function failed
	16	DSPSERV Delete failed

Note: These return codes and reason codes are described in *z/OS MVS Programming: Authorized Assembler Services Guide*.

ICH14059I **Class *class-name* was not activated by the SETROPTS CLASSACT(*) command.**

Explanation: The SETROPTS CLASSACT(*) command was issued and the class indicated in the message has a default return code of 8 in the class descriptor table. This class should be activated explicitly.

System Action: The class indicated in the message was not affected by the SETROPTS command.

User Response: If you want this class to be activated, ensure that profiles have been defined for this class, then use SETROPTS *class-name* to activate it.

If you do not want this class to be activated, issue a SETROPTS LIST command to ensure that the class was not activated by means of a shared POSIT value. If the class has been activated, contact your system programmer.

System Programmer Response: See *z/OS Security Server RACF Macros and Interfaces* for an explanation of defining a class with shared POSIT values.

ICH14060I **Incomplete specification of *keyword* keyword. Keyword ignored.**

Explanation: The syntax of the keyword *keyword* was not completely specified.

System Action: The keyword is ignored by the SETROPTS command.

User Response: Respecify the keyword with the correct syntax.

ICH14061I **SETROPTS command processing other than LIST is not permitted while system is running in read-only mode. Any keyword other than LIST is ignored.**

Explanation: A SETROPTS command other than LIST was entered. The system is in read-only mode, and LIST is the only keyword allowed.

System Action: Any SETROPTS keywords other than LIST are ignored.

System Programmer Response: To successfully issue a SETROPTS command, you can:

- Issue SETROPTS command from another system that is not in read-only mode.
- Issue RVAR DATASHARE to change the mode of all systems to data sharing mode and reissue the SETROPTS command.
- Issue RVAR NODATASHARE to change the mode of all systems to non-data sharing mode and reissue the SETROPTS command.

ICH14062I **Coupling facility failure occurred during {primary | backup} data set processing. Command processing stops.**

Explanation: An error occurred when accessing the coupling facility.

System Action: SETROPTS processing ends abnormally.

System Programmer Response: Check the information specified in message IRRX016I, which is issued to the system console. Changes requested via

ICH14063I • ICH14068I

SETROPTS may not have taken effect. Verify these changes after the coupling facility related error has been corrected. Reissue the SETROPTS command again as necessary.

ICH14063I SETROPTS command complete.

Explanation: The system is enabled for sysplex communication and the SETROPTS command for coordinated requests has completed. If this message is preceded by other messages, refer to those messages for appropriate action. Other SETROPTS commands can now be processed.

ICH14064I ALESERV ADD function failed with return code X'*retcode*' during SETROPTS *raclist-type* command processing for class *classname*.

Explanation: The system is enabled for sysplex communication and a SETROPTS RACLIST or SETROPTS RACLIST REFRESH command encountered an ALESERV ADD error while trying to obtain an ALET during the creation of a new data space. This message occur only on the peer system.

Note: This message appears in uppercase when issued to the operator console.

System Action: Command processing stops on all systems if the coordinating system is running in data sharing mode. Otherwise, processing continues on systems where the command can be processed successfully.

User Response: If the SETROPTS command failed, reissue the command. If the problem persists, report this message along with the return code to the system programmer.

System Programmer Response: See *z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN* for the description of the return codes for the ALESERV macro. If necessary, contact the IBM support center.

ICH14065I Class *classname* not defined in class descriptor table (CDT).

Explanation: The system is enabled for sysplex communication and a coordinated SETROPTS command was issued on another system in the sysplex to perform some type of operation on the specified class. That class is not defined in the class descriptor table on this system.

Note: This message appears in uppercase when issued to the operator console.

System Action: The command is ignored on this system but is processed on other systems where *classname* is defined in the class descriptor table.

User Response: Check with your system programmer to determine if the class should be added to the class descriptor table.

ICH14066I Error refreshing global access table for class *classname*.

Explanation: The system is enabled for sysplex communication and an error occurred when RACF attempted to update the global access table on this system.

Note: This message appears in uppercase when issued to the operator console.

System Action: If the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues on systems where the command can be processed successfully.

ICH14067I Coordinated SETROPTS operation failed on one or more members of the RACF group. Command processing continues.

Explanation: The system is enabled for sysplex communication and a SETROPTS command was propagated to other members in the sysplex. One or more of these members failed to execute the command, but command processing continues.

User Response: Check the system log for message IRRX006I to identify the members that experienced the failure. Consult the system logs for each failing member for messages or additional information.

ICH14068I Coordinated SETROPTS operation failed on one or more members of the RACF group. Command processing stops.

Explanation: The system is enabled for sysplex communication and a SETROPTS command was propagated to other members in the sysplex. One or more of these members failed to execute the command, and command processing stopped for the class named in the message sent to the peer member, and continues for the other classes, if any, in the scope of the SETROPTS command.

User Response: Check the system log for message IRRX006I to identify the peer members that experienced the failure. Consult the system logs for each failing peer member for messages or additional information.

ICH14069I Error refreshing program access table.

Explanation: The system is enabled for sysplex communication and an error occurred when RACF attempted to refresh the program access table on this system.

Note: This message appears in uppercase when issued to the operator console.

System Action: If the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues on systems where the command can be processed successfully.

ICH14070I SETROPTS *raclist-type* had no effect on class *classname*.

Explanation: One of the following occurred:

- A SETROPTS RACLIST was issued and this class was already SETROPTS RACLISTed.
- A SETROPTS RACLIST REFRESH or SETROPTS NORACLIST command was issued and this class was not RACLISTed by either a SETROPTS RACLIST command or a RACROUTE REQUEST=LIST,GLOBAL=YES request.

In either case, if this system is enabled for sysplex communication, this message applies to all members of the sysplex.

System Action: The command had no effect on this class.

User Response: Check that the *classname* specified on the original command is the class you want. SETROPTS *raclist-type* commands process all the classes with the same posit as the class specified in the command. Therefore, *classname* in this message may not be the class specified in the command. Issue a SETROPTS LIST command to verify classes that are RACLISTed.

ICH14071I SETROPTS *raclist-type* had no effect on class *classname* except to alter RACGLIST profiles.

Explanation: One of the following occurred:

- A SETROPTS RACLIST REFRESH was issued and RACF found that the class was not RACLISTed by either SETROPTS or RACROUTE REQUEST=LIST,GLOBAL=YES, so no data space was refreshed. However, the RACGLIST *classname_00001-0000n* profiles were updated from *classname* profiles on the RACF database.
- A SETROPTS NORACLIST was issued and RACF found that the class was not RACLISTed by either SETROPTS or RACROUTE REQUEST=LIST,

GLOBAL=YES, so no data space was deleted. However, the RACGLIST *classname_00001-0000n* profiles were deleted.

In either case, if this system is enabled for sysplex communication, this message applies to all members of the sysplex.

User Response: Check that the *classname* specified on the original command is the class you want. SETROPTS *raclist-type* commands process all the classes with the same posit value as the class specified in the command. Therefore, *classname* in this message may not be the class specified in the command. Issue a SETROPTS LIST command to verify classes that are RACLISTed.

ICH14072I The SETROPTS command failed to propagate to other members in the sysplex. Command processing stops.

Explanation: RACF is enabled for sysplex communication and XCF encountered an error while attempting to propagate the command to the other members of the sysplex. One or more of these members failed to process the SETROPTS command and command processing stopped. An attempt was made to back out the command where possible. The in-storage profiles might be out of synch with others in the sysplex.

User Response: Report this message to your system programmer.

System Programmer Response: Check the system logs of the member where the command was issued for additional information. Save dumps and system logs. Refer to the MVS documentation on XCF failures to determine the problem. After the problem has been resolved, reissue the SETROPTS command. If necessary, contact your IBM support center.

ICH14073I WARNING: Class *class-name* was activated by the SETROPTS command. Authorization checks might fail.

Explanation: As a result of a SETROPTS CLASSACT command, class *class-name* was activated. This class has a default return code of 8 in the class descriptor table and has no profiles. All authorization checks for resources in this class will fail unless overridden by an installation exit.

System Action: The class, *class-name*, was activated. Other classes with the same POSIT value, if any exist, were also activated. No message is issued for those classes.

User Response: If you want class *class-name* to remain active, be sure that profiles are not required for this class or that the appropriate installation exits are installed (for example, ICHRCX01 or ICHRCX02).

Because authorization checks to any resource in the

ICH14074I • ICH14077I

class fail without appropriate exits, you might want to deactivate the class by issuing the SETROPTS NOCLASSACT(*class-name*) command.

System Programmer Response: See *z/OS Security Server RACF Macros and Interfaces* for an explanation of shared POSIT values, for instructions on how to change the POSIT value for a class, or for an explanation of default return code 8.

ICH14074I WARNING: Generic profiles created with EGN in effect might not protect resources when NOEGN is in effect.

Explanation: EGN (enhanced generic naming) was in effect and NOEGN was specified on the SETROPTS command. Some generic profiles containing an * or ** that were created while EGN was in effect will not protect any resources when NOEGN is in effect. For example, profile 'USER1.AB.**CD' protects USER1's data sets AB.CD and AB.EF.CD when EGN is in effect. 'USER2.GH.*' protects USER2's data sets GH.IJ and GH.KL. The profiles, created when EGN was in effect, are not recognized when NOEGN is in effect and do not protect any resources.

System Action: The command proceeds and NOEGN is placed in effect.

User Response: Do one of the following:

- If the change to NOEGN caused some resources to become unprotected, issue SETROPTS EGN to place EGN in effect .
- If placing NOEGN in effect does not leave resources unprotected, no action is required.

Contact your system administrator if you need help determining if any resources need to be protected.

RACF Security Administrator Response: Be sure that no resources are left unprotected when NOEGN is placed in effect. Use the SEARCH and LISTDSD commands to determine what profiles are defined and which profile protects a particular resource. Refer to "Naming Considerations For Resource Profiles" in *z/OS Security Server RACF Command Language Reference* for a discussion of the differences between generic profile protection with EGN and NOEGN.

ICH14075I SETROPTS keyword had no effect on class classname.

Explanation: SETROPTS *keyword* was issued for the class *classname*. However, this class does not support generic profile checking, or generic profile command processing, so the *keyword* option cannot be activated for this class.

System Action: RACF ignores this class. Command processing continues with the next operand.

ICH14076I The option-name option cannot be activated because the SECLABEL class is inactive.

Explanation: The SETROPTS command was issued for an option that requires the SECLABEL class be active, but the SECLABEL class is not active, or is being deactivated by this SETROPTS command.

System Action: The option specified by option-name was not activated.

User Response: Reissue the command after activating the SECLABEL class.

ICH14077I Active multi-level security options do not allow the deactivation of the SECLABEL class.

Explanation: The SETROPTS command was issued to deactivate the SECLABEL class, but one or more options requiring that this class be active such as MLS or MLACTIVE are currently in effect.

System Action: The SECLABEL class was not deactivated by the SETROPTS command.

User Response: Deactivate the options and try again.

RVARY command messages

ICH15001I REQUEST DENIED - RACF PERMANENTLY INACTIVE

Explanation: The RACF CVT (RCVT) indicates that RACF is not active.

System Action: Command processing stops.

User Response: Issue this command after RACF is initialized.

ICH15002I DATASET *dsname* ALREADY IN REQUESTED STATE

Explanation: The user requested that the indicated data set be made active and the data set is currently active, or the user requested that the indicated data set be made inactive and the data set is currently inactive.

System Action: Command processing continues with the next data set name in the list.

ICH15004I BACKUP DATASET CAN NOT BE SWITCHED; *dsname* IGNORED

Explanation: The user attempted to switch the indicated data set with its backup but the indicated data set is currently a backup data set.

System Action: Command processing continues with the next data set name in the list.

ICH15005I PRIMARY MASTER DATASET ACTIVE; NOCLASSACT/NOTAPE OPERAND IGNORED

Explanation: The user specified either the NOCLASSACT operand or the NOTAPE operand while the primary master data set was active.

System Action: RACF ignores the operand. Command processing continues with the next operand.

ICH15006I DATASET *dsname* HAS NO BACKUP; DATASET NOT SWITCHED

Explanation: The user attempted to switch the indicated data set with its backup but the indicated data set currently has no backup.

System Action: Command processing continues with the next data set name in the list.

ICH15007I CHANGES TO RACF STATUS DENIED. OPERATOR ENTERED INCORRECT PASSWORD

Explanation: The operator entered an incorrect password in response to message ICH702A.

System Action: The status of RACF remains unchanged.

User Response: Provide the operator with the correct password. If you were attempting a RVARY ACTIVE, RVARY NODATASHARE, or RVARY SWITCH command, reissue the command from a console with master authority and instruct the operator to reply YES.

ICH15008I COMMAND PROCESSING TERMINATED. ERROR ENCOUNTERED DURING PASSWORD ENCRYPTION.

Explanation: To approve the user's issuance of the RVARY command, the operator must enter an installation-defined password. If RACF fails to encrypt this password at the time the operator issues it, you receive this message.

System Action: Command processing stops.

User Response: Provide the operator with the correct password. If you were attempting a RVARY ACTIVE, RVARY NODATASHARE, or RVARY SWITCH command, reissue the command from a console with master authority and instruct the operator to reply YES.

Report this message to your system programmer.

Programmer Response: IPL again and try the command again.

Problem Determination: If this message recurs, call your IBM support center.

ICH15009I ERROR ENCOUNTERED WHEN ATTEMPTING REQUESTED OPERATION, OPERATION NOT PERFORMED.

Explanation: An error occurred during RVARY processing.

System Action: Command processing stops.

User Response: Report this message to your system programmer.

Programmer Response: IPL again and try the command again.

Problem Determination: If this message recurs, call your IBM support center.

ICH15010I ERROR WHEN INVOKING RACF DATASET ALLOCATION/DEALLOCATION OPERATION, TRY AGAIN. IF THIS PROBLEM PERSISTS, CALL OPERATOR.

Explanation: An error occurred while attempting to allocate or deallocate a RACF data set.

System Action: Command processing stops.

ICH15011I • ICH15021I

User Response: Report this message to your operator or system programmer.

Operator Response: Report this message to your system programmer.

Programmer Response: IPL again and try the command again.

Problem Determination: If this message recurs, call your IBM support center.

ICH15011I RVARY SWITCH DENIED. ALL REQUIRED BACKUP DATA SETS MUST BE ACTIVE BEFORE ISSUING THE SWITCH COMMAND.

Explanation: The RVARY SWITCH command was issued when one or more of the data sets to be switched was not active.

System Action: The command is not processed.

Operator Response: Notify the system programmer.

Programmer Response: All backup data sets must be active when attempting an RVARY SWITCH command. Activate the backup data sets (using the RVARY ACTIVE command) and then switch.

ICH15013I RACF DATABASE STATUS:

Explanation: This message begins a display of RACF database status information in response to issuing the RVARY LIST command, or any RVARY command in which the NOLIST operand is not in effect.

Destination: Descriptor code 6. Routing code 2.

ICH15014I INVALID KEYWORD ENCOUNTERED FOR RVARY

Explanation: An RVARY command was issued with an incorrect keyword specified.

Destination: Descriptor code 6. Routing code 2.

ICH15017I RACF IS NOT ENABLED FOR SYSPLEX COMMUNICATIONS. DATASHARE OR NODATASHARE KEYWORDS MAY NOT BE SPECIFIED.

Explanation: The DATASHARE and NODATASHARE keywords cannot be specified when RACF is not enabled for sysplex communications.

System Action: RACF does not process the command.

ICH15018I RACF DATA SHARING GROUP *group-name* ALREADY IN NON-DATA SHARING MODE. NODATASHARE KEYWORD MAY NOT BE SPECIFIED.

Explanation: The RACF data sharing group is already in non-data sharing mode, so RVARY NODATASHARE cannot be specified.

System Action: RACF does not process the command.

ICH15019I INITIATING PROPAGATION OF RVARY COMMAND TO MEMBERS OF RACF DATA SHARING GROUP *group-name* [IN RESPONSE TO A REBUILD REQUEST].

Explanation: RACF is initiating the propagation of the RVARY command to the other members of the RACF data sharing group *group-name*. Propagation will be complete when message ICH15020I is issued and subsequent RVARY commands will then be processed.

System Action: The command is propagated.

ICH15020I RVARY COMMAND [INITIATED IN RESPONSE TO THE REBUILD REQUEST] HAS FINISHED PROCESSING.

Explanation: The RVARY command processing has completed. If this message is preceded by other messages, refer to those messages for appropriate action. Subsequent RVARY commands can now be processed.

System Action: RACF continues operation.

Operator Response: RVARY processing was not completely successful if this message is preceded by any of the following messages:

ICH15009I IRRX003A
ICH15010I IRRX009I
ICH15011I IRRX010I
ICH15021I IRRX011A
ICH15022I IRRX012I
ICH15023I IRRX013A
ICH15024I
ICH15025I
ICH15026I

Refer to those messages for further action.

ICH15021I UNABLE TO OBTAIN SERIALIZATION FOR THE REQUESTED COMMAND. THE COMMAND IS NOT PERFORMED.

Explanation: RACF was unable to obtain serialization to perform the requested command.

System Action: RACF does not process the command.

User Response: Report this message to your system programmer.

System Programmer Response: Check the system log for serialization-related messages to determine and correct the problem.

ICH15022I ONE OR MORE MEMBERS OF THE RACF DATA SHARING GROUP FAILED TO PROCESS THE PROPAGATED RVARY COMMAND.

Explanation: RACF is enabled for sysplex communication and propagated the command to the other members of the RACF data sharing group. However, one or more members of the group failed to process the command as expected.

System Action: Command propagation completes. One or more members had a processing error.

User Response: Report this message to your system programmer.

System Programmer Response: Check the system log for IRRX006I messages. If found, these messages identify the members who experienced the failure. Obtain the system logs for each failing member to determine additional RACF messages that might have been issued. RVARY LIST may also be used to determine if the status of the failing members is different from what was expected. If you do not find any IRRX006I messages, an XCF failure could have occurred during processing. Any member that leaves the RACF data sharing group because of this failure issues the ICH501I message.

ICH15023I ERROR OCCURRED WHILE INVOKING RVARY COMMAND.

Explanation: An internal error occurred during an attempt to process an RVARY command.

System Action: RACF does not process the command.

User Response: Report this message to your system programmer.

System Programmer Response: Save dumps and the system log. Contact your IBM support center. An IPL may be necessary.

ICH15024I RACF IS PROCESSING A PRIOR RVARY COMMAND. [RE-ISSUE THE COMMAND.]

Explanation: RACF has not completed processing of a prior RVARY command.

System Action: RACF does not process the command.

User Response: For rebuild, issue the RVARY NODATASHARE command followed by an RVARY

DATASHARE command. Otherwise, reissue the original RVARY command. If this message persists, contact your system programmer.

System Programmer Response: Use the MVS DUMP command to obtain a dump of the Master, RACFDS, and RACF subsystem address spaces and call your IBM support center. An IPL may be necessary.

ICH15025I THE RVARY COMMAND WAS NOT PROCESSED BY ANY MEMBER OF THE RACF DATA SHARING GROUP.

Explanation: RACF is enabled for sysplex communication and attempted to propagate the command to the other members of the RACF data sharing group. However, none of the members of the group processed the command. If RVARY propagation was interrupted by an XCF failure, it is possible that some members of the RACF data sharing group might have quiesced activity against the RACF database in preparation for processing the command. These members cannot use the RACF database until the command is reissued and processing is complete.

System Action: RACF does not process the command.

User Response: Report this message to your system programmer.

System Programmer Response: Check the system log for additional information, such as XCF failures, IRRX006I messages, or other related RACF messages. Correct the problem and reissue the command.

ICH15026I A SEVERE ERROR OCCURRED DURING THE PROPAGATION OF THE RVARY COMMAND.

Explanation: RACF detected a severe error while attempting to propagate an RVARY command.

System Action: The RACF data sharing group has attempted to process the command, but this member experienced a severe error. In order to prevent damage to the RACF database and to ensure that other members of the RACF data sharing group are not affected by the error, this member has entered permanent failsoft mode and has been removed from the group.

User Response: Report this message to your system programmer.

System Programmer Response: Check the system log for additional information. Save dumps and the system log. Refer to the MVS documentation on XCF failures. If necessary, contact your IBM support center. An IPL is required to return this member to an active state.

ICH15027I • ICH15029I

ICH15027I RVARY COMMAND REJECTED. ROUTE IS ONLY ALLOWED FOR RVARY LIST. RE-ISSUE COMMAND TO A SINGLE SYSTEM ONLY.

Explanation: The RVARY command was prefixed with the MVS ROUTE command, directing the command to multiple members of the RACF data sharing group. This is allowed only for RVARY LIST, with no additional RVARY keywords specified. If you reissue the RVARY command to a single member only, RACF propagates the command to the other members of the group.

System Action: RACF does not process the command.

Operator Response: Reissue the command to a single member.

ICH15028I MVS RELEASE LEVEL IS NOT AT LEAST RELEASE 5.1. DATASHARE OR NODATASHARE KEYWORDS CANNOT BE SPECIFIED.

Explanation: All members of the RACF data sharing group must be at MVS 5.1 or above for a RVARY DATASHARE or RVARY NODATASHARE command to function. This message indicates that the member to which the command was issued was not at the sufficient level.

System Action: RACF does not process the command.

System Programmer Response: If data sharing is desired, all the members of the RACF data sharing group must be upgraded to MVS 5.1 or above.

ICH15029I THIS MEMBER OF THE RACF DATA SHARING GROUP IS IN READ-ONLY MODE. THE SWITCH KEYWORD MAY NOT BE SPECIFIED.

Explanation: This member of the RACF data sharing group is in read-only mode, so RVARY SWITCH cannot be specified.

System Action: RACF does not process the command.

User Response: Reissue the command from a member of the RACF data sharing group that is not in read-only mode. If all members are in read-only mode, issue the RVARY NODATASHARE command, followed by the RVARY SWITCH command.

ALTGROUP command messages

ICH20002I NOT AUTHORIZED TO ALTER
group-name

Explanation: You do not have sufficient authority to alter the group indicated in the message.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH20003I NOT AUTHORIZED TO SPECIFY
OWNER

Explanation: You do not have sufficient authority to specify the OWNER operand.

System Action: Processing continues with the owner field unchanged.

User Response: See your RACF security administrator.

ICH20004I ERROR FOUND IN GROUP TREE
STRUCTURE

Explanation: An inconsistency or error was found in the group tree structure while processing the ALTGROUP command.

System Action: Command processing stops.

User Response: Use the LISTGRP command to list groups in the superior group tree structure, looking in particular for disagreements between superior groups and subgroups.

ICH20005I INSUFFICIENT AUTHORITY TO
[SUPERIOR GROUP OF] *group-name*

Explanation: You do not have sufficient authority to change the superior group indicated in the message.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH20006I xxxxxxxx CANNOT BE A SUPERIOR
GROUP OF yyyyyyyy

Explanation: The command requested that group xxxxxxxx be made the superior group of yyyyyyyy. However, group yyyyyyyy is already above group xxxxxxxx in the group hierarchy and the result would be a circular definition that is invalid.

System Action: The subgroup list for group xxxxxxxx is not changed. Command processing stops.

ICH20007I {TERMUACC | NOTERMUACC} NOT
ALTERED FOR GROUP *group-name*

Explanation: An error occurred while altering the TERMUACC or NOTERMUACC operand for the group indicated in the message. The TERMUACC and NOTERMUACC indicators in the group profile and connect entries are not updated.

System Action: Command processing continues with the next operand.

ICH20008I {TERMUACC | NOTERMUACC} NOT
ALTERED FOR {USER *userid* | ANY
USERS}

Explanation: An error occurred during one of the following:

- Retrieving the access list of all users connected to the group (indicated by ANY USERS)
- Altering the TERMUACC or NOTERMUACC indicator in the connect profile for user *userid*

System Action: The TERMUACC or NOTERMUACC indicator in the group profile was altered to the value specified on the command. If the error occurred while retrieving the access list, command processing stops. If the error occurred while altering a connect profile for user *userid*, command processing continues with the next user ID in the access list.

ICH20009I *group-name* NOT ALTERED,
PROGRAMMING LIMIT EXCEEDED

Explanation: While searching the index structure for the superior group of the group specified, more than 398 superior groups were found. This exceeds the RACF command limit.

System Action: RACF ignores the SUBGROUP operand. Command processing continues with the next operand.

ICH20010I NOT AUTHORIZED TO ISSUE
ALTGROUP

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is

ICH20011I • ICH20019I

not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH20011I COMMAND ENDED DUE TO ERROR

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH20012I RECOVERY UNSUCCESSFUL

Explanation: As issued, the ALTGROUP command began to update more than one profile in the RACF database. However, a system or RACF failure occurred during command processing.

System Action: To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes could be backed out. This message follows message ICH20013I.

User Response: Report this message and the exact text of message ICH20013I to your system programmer.

Problem Determination: The RACF utility programs may be needed to correct the RACF database.

ICH20013I *group-name* NOT ALTERED

-or-
GROUP(S) NOT ALTERED

Explanation: An error occurred during ALTGROUP command processing.

System Action: The group indicated in the message was not altered.

ICH20014I OWNER NOT ALTERED FOR *group-name*

Explanation: An error occurred while processing the owner field specified in the OWNER operand.

System Action: RACF does not alter the owner field.

Command continues processing with the next operand.

ICH20015I SUPGROUP NOT ALTERED FOR *group-name*

Explanation: An error occurred while processing the superior group field specified in the SUPGROUP operand.

System Action: The superior group field is not altered and the command continues processing with the next operand.

ICH20016I NOT AUTHORIZED TO SPECIFY THE DATA OR NODATA KEYWORDS

Explanation: You do not have sufficient authority to alter the installation-defined data in the group profile.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH20017I NOT AUTHORIZED TO SPECIFY THE MODEL OR NOMODEL KEYWORDS

Explanation: You do not have sufficient authority to specify the MODEL or NOMODEL operand on the ALTGROUP command.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH20018I WARNING, UNABLE TO LOCATE THE MODEL PROFILE FOR *dsname*

Explanation: You have specified a model profile data set name that cannot be found on the RACF database. For modeling to be effective for this data set name, a data set profile must first be created.

System Action: RACF adds the data set name you specified to the group profile in anticipation that profile information for this name will be completed (using the ADDSD command) at a later time.

RACF continues to process the ALTGROUP command.

ICH20019I UNABLE TO LOCATE *group-name*

Explanation: The group indicated in the message could not be found in the RACF database.

System Action: Command processing continues with the next group name in the list.

**ICH20020I OWNER-GROUP AND SUPERIOR
GROUP MUST BE THE SAME FOR
GROUP *group-name***

Explanation: When the owner of a group is another group, the owning group and the superior group must be the same. This message is followed by message ICH20014I or message ICH20015I, or both.

**ICH20021I NOT AUTHORIZED TO ALTER
SEGMENT FOR GROUP *group-name***

Explanation: You are not authorized to change the segment for the specified group.

System Action: Command processing ends with no update to the group profile.

User Response: See your RACF security administrator for authority to the segment of this group profile.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add segment information. For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

**ICH20022I DFP SEGMENT NOT ALTERED FOR
GROUP *group-name***

Explanation: You are not authorized to change the DFP segment for the specified group.

System Action: Command processing stops with no update to the group profile.

User Response: See your RACF security administrator for authority to the DFP segment of this group profile.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

ALTUSER command messages

ICH21001I COMMAND ENDED DUE TO ERROR UNABLE TO PROMPT FOR OIDCARD

Explanation: You specified the OIDCARD operand, but TSO/E was unable to prompt you to enter the operator identification card.

System Action: Command processing stops.

User Response: Be sure you are executing the command in the foreground and in prompt mode.

ICH21002I COMMAND ENDED DUE TO ERROR UNABLE TO ESTABLISH ESTAE

Explanation: An ESTAE recovery environment could not be established.

System Action: Command processing stops.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH21003I COMMAND ENDED DUE TO ERROR PUTGET ERROR RETURN CODE IS *xx*

Explanation: You specified the OIDCARD operand, but the TSO/E PUTGET service routine failed with a return code indicated by *xx* while trying to read the operator identification card. For an explanation of the return code, see *z/OS TSO/E Programming Services*. For the order number of the documentation you need, see *z/OS TSO/E General Information*.

ICH21004I {*userid* | DFLTGRP | OWNER | USER} NOT ALTERED

Explanation: An error occurred during RACF processing.

System Action: If a user ID appears in the message, the user profile was not changed. If USER appears, the error occurred before a particular user ID could be determined. Otherwise, the DFLTGRP or OWNER fields were not altered.

User Response: One of the following:

- If DFLTGRP appears in the message, the user specified on the ALTUSER command was not already connected to the group specified on the DFLTGRP operand. Use the CONNECT command to connect

the user to the group (with the desired group authority), then issue the ALTUSER command with DFLTGRP specified again.

- If OWNER appears in the message, there is no profile (user or group, as appropriate) for the owner specified on the ALTUSER command.

ICH21005I NOT AUTHORIZED TO SPECIFY *operand*, OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the indicated operand.

System Action: RACF ignores the operand and continues processing with the next operand.

User Response: See your RACF security administrator.

ICH21006I AUTHORITY SPECIFIED GREATER THAN THE COMMAND USER

Explanation: You have CONNECT authority and cannot specify JOIN authority. The other operands were modified.

User Response: See your RACF security administrator.

ICH21007I EXPIRED/NOEXPIRED OPERAND IGNORED

Explanation: You specified the EXPIRED or NOEXPIRED operand but the PASSWORD operand was not specified on the command. EXPIRED and NOEXPIRED are valid only if specified with the PASSWORD operand.

System Action: RACF ignores the operand and continues command processing with the next operand.

ICH21008I NOT AUTHORIZED TO SPECIFY CLAUTH/NOCLAUTH FOR {USER, TAPEVOL, DASDVOL, TERMINAL}, CLASS IGNORED

Explanation: You do not have sufficient authority to specify the CLAUTH or NOCLAUTH operands for the indicated class.

System Action: RACF ignores the class and continues command processing with the next class specified.

User Response: See your RACF security administrator.

ICH21009I UNABLE TO LOCATE *userid*

Explanation: The indicated user ID could not be found in the RACF database.

System Action: Command processing stops.

ICH21010I NOT AUTHORIZED TO ISSUE ALTUSER

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH21011I {AUTHORITY | UACC} NOT ALTERED

Explanation: An error occurred during ALTUSER command processing.

System Action: The AUTHORITY or UACC fields are not altered.

ICH21012I AUTHORIZED TO ISSUE ONLY UAUDIT/NOUAUDIT FOR *userid*; REMAINING OPERANDS IGNORED

Explanation: You specified operands in addition to UAUDIT or NOUAUDIT, but for the indicated user ID, you are only authorized to specify the UAUDIT or NOUAUDIT operands.

System Action: All operands other than UAUDIT or NOUAUDIT are ignored.

User Response: See your RACF security administrator.

ICH21013A ENTER OPERATOR IDENTIFICATION CARD

Explanation: You have specified the OIDCARD operand. This message is requesting that you enter the operator identification card for the user being altered so that the information on it can be put into the user's profile.

System Action: Command processing waits for you to enter the operator identification card.

**ICH21014I COMMAND ENDED DUE TO ERROR
TERMINAL TYPE NOT SUPPORTED**

Explanation: You specified the OIDCARD operand, but when the operator identification card was entered, it could not be verified because it was entered on a terminal that is not supported.

System Action: The ALTUSER command stops processing.

**ICH21015I CLASS *class-name* AND REMAINING
CLASSES NOT ALTERED FOR
CLAUTH/NOCLAUTH**

Explanation: The indicated class and all remaining class names in the CLAUTH/NOCLAUTH list were not added to or deleted from the list of authorized classes in the user profile because an error occurred in the RACF manager.

System Action: A RACF-manager error message precedes this message and explains the error. Other operands on the command have been processed.

**ICH21016I PASSWORD CHANGE FOR '*id*'
SUPPRESSED BY INSTALLATION
PASSWORD EXIT**

Explanation: The proposed password, as specified in the PASSWORD operand on the ALTUSER command, does not obey the syntax rules of the installation. (These rules were specified by the PASSWORD keyword, RULE*n* option, on the SETROPTS command.)

System Action: Command processing stops.

User Response: See your RACF security administrator for the rules regarding new passwords.

**ICH21017I NOT AUTHORIZED TO SPECIFY
MODEL/NOMODEL, OPERAND
IGNORED**

Explanation: You do not have sufficient authority to specify MODEL or NOMODEL on the ALTUSER command.

System Action: RACF ignores the operand and continues command processing with the next operand.

User Response: See your RACF security administrator.

**ICH21018I WARNING, UNABLE TO LOCATE THE
MODEL PROFILE FOR *dsname***

Explanation: You have specified a model profile data set name that cannot be found on the RACF database. For modeling to be effective for this data set name, a data set profile must first be created.

System Action: RACF adds the data set name you specified to the user profile in anticipation that profile

ICH21019I • ICH21031I

information for this name will be completed (using the ADDSD command) at a later time. RACF continues to process the ALTUSER command.

ICH21019I 'RESUME' IGNORED. *userid* NOT CURRENTLY REVOKED

Explanation: The indicated user ID is not currently revoked.

System Action: RACF ignores the specification of a future date with the RESUME operand.

ICH21020I *category* ALREADY DEFINED TO *profile-name*

Explanation: The specified category has already been defined in this profile.

System Action: RACF ignores the category and continues command processing with the next operand.

ICH21021I *category* NOT DEFINED TO *profile-name*

Explanation: Because the specified category has not been defined in this profile, RACF cannot delete it.

System Action: RACF ignores the category and continues command processing with the next operand.

ICH21022I 'REVOKE' IGNORED. *userid* IS CURRENTLY REVOKED

Explanation: REVOKE was specified with a date, but the user is already revoked.

System Action: RACF ignores REVOKE processing and continues command processing with the next operand.

ICH21023I COMMAND PROCESSING TERMINATED. NO {SECLEVELS | CATEGORIES} FOUND

Explanation: RACF could not validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System Action: Command processing stops.

ICH21026I NOT AUTHORIZED TO SPECIFIED FIELD(S) IN *segment-name* SEGMENT

Explanation: You are not authorized to update the fields specified on the ALTUSER command in segment *segment-name*.

System Action: Command processing stops with no update to the RACF database.

User Response: See your RACF security

administrator for authority to the DFP segment of this group profile.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

ICH21027I COMMAND PROCESSING COMPLETED BUT UNABLE TO UPDATE 'SYS1.BROADCAST'.

Explanation: The command you issued has been completed; however, your attempt to change the TSO/E data set SYS1.BROADCAST has failed.

ICH21028I *segment-name* OPERAND NOT PROCESSED

Explanation: You are not authorized to change the specified segment.

System Action: None of the operands for this segment are processed.

User Response: See your RACF security administrator for authority to this segment.

ICH21029I CONFLICT BETWEEN SIZE AND MAXSIZE. OPERAND IS IGNORED.

Explanation: The SIZE and MAXSIZE operands differ.

System Action: Both operands are ignored.

ICH21030I SIZE SPECIFIED GREATER THAN MAXSIZE. SIZE ADJUSTED EQUAL TO MAXSIZE.

Explanation: The specified size is greater than the maximum allowable size, as specified on the MAXSIZE operand.

System Action: RACF adjusts the size to equal the MAXSIZE operand.

User Response: You can adjust the SIZE and MAXSIZE operands using the ALTUSER command.

ICH21031I ALTUSER failed. NOSECLABEL is not allowed under the current RACF options.

Explanation: NOSECLABEL operand was specified on the ALTUSER command, and SETROPTS MLACTIVE is on.

System Action: Command processing stops.

User Response: Correct the command.

ICH21032I **ALTUSER failed. SECLABEL**
seclabel-name is not currently defined
 to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System Action: Command processing stops.

User Response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, define a profile of that name in the SECLABEL class. If you cannot define such a profile, report the exact text of this message to your RACF security administrator.

ICH21033I **ALTUSER failed. User is not connected**
 to group *group-name*

Explanation: The indicated group name was specified in the DFLTGRP operand, but the user is not yet connected to the group.

System Action: The command continues, but the DFLTGRP is not updated in the user profile.

User Response: Correct the DFLTGRP operand, or use the CONNECT operand to connect the user to the specified group name and issue the command again.

ICH21034I **PASSWORD CHANGE REJECTED BY**
INSTALLATION SYNTAX RULES

Explanation: You specified a potential password that does not adhere to the syntax rules that are in effect for your installation.

System Action: RACF ignores the operand and continues command processing with the next operand.

User Response: See your RACF security administrator for the syntax rules for passwords.

ICH21035I **User *username* is assigned an OMVS**
UID, but default group *grpname* does
not have a GID. Processing continues.

Explanation: This is a warning message that gets issued if a user with an OMVS UID gets changed and has a default group which does not have a GID.

User Response: This usage violates documented rules. Either the default group should be assigned a GID, or the UID should be removed from the user profile.

RACF Security Administrator Response: Follow documented guidelines to assure that default groups for (OMVS users with UIDs) have GIDs assigned.

ALTDSD command messages

ICH22001I *profile-name* NOT DEFINED TO RACF

Explanation: The profile indicated in the message is not defined to RACF and cannot be altered.

System Action: Processing continues with the next profile name.

Note: If you enter the ALTDSD command for a fully qualified generic profile (one whose name has no generic characters), but you do not specify the GENERIC operand, RACF issues this message. This occurs because, without the GENERIC operand, RACF looks for a discrete profile of that name. For example, if there is a fully qualified generic profile named ABC.DATA, and you enter the following command:

```
ALTDSD 'ABC.DATA'
```

RACF looks for a discrete profile named ABC.DATA and, if there is none, issues this message (ICH22001I ABC.DATA NOT DEFINED TO RACF). To identify for RACF the generic profile, specify the GENERIC operand as follows:

```
ALTDSD 'ABC.DATA' GENERIC
```

ICH22002I NOT AUTHORIZED TO SPECIFY OWNER

Explanation: You do not have sufficient authority to specify the OWNER operand.

System Action: The owner field is not changed. Processing continues with the next operand of the ALTDSD command.

User Response: See your RACF security administrator.

ICH22003I NOT AUTHORIZED TO ISSUE ALTDSD

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command,

see *z/OS Security Server RACF Command Language Reference*.

ICH22004I COMMAND ENDED DUE TO ERROR

Explanation: A RACF-manager error occurred. This message is accompanied by a message explaining the error.

ICH22005I NOT AUTHORIZED TO ALTER *profile-name*

Explanation: You are not authorized to change the indicated profile.

System Action: The profile is not altered. Processing continues with the next profile.

User Response: See the owner of the profile or your RACF security administrator. To display the owner of the profile, use the LISTDSD command.

ICH22006I OWNER SPECIFIED NOT DEFINED TO RACF

Explanation: The user ID or group name specified on the OWNER operand is not a RACF-defined user.

System Action: Command processing continues with the next operand.

ICH22007I OWNER SPECIFIED NOT AUTHORIZED TO GROUP

Explanation: The user ID specified on the OWNER operand does not have sufficient authority to the group whose name is the first level qualifier of the data set being altered.

System Action: Command processing continues with the next operand.

User Response: See your RACF security administrator.

ICH22008I ADDVOL/DELVOL NOT ALLOWED FOR VSAM/MODEL DATASET

Explanation: The ADDVOL and DELVOL operands apply only to non-VSAM data sets.

System Action: The ADDVOL or DELVOL operand is ignored. Command processing continues with the next operand.

ICH22009I VOLUME SPECIFIED ALREADY EXISTS IN DATASET PROFILE

Explanation: The ADDVOL or ALTVOL operand was specified which requests a volume to be added to the

data set profile but the volume already exists in the profile.

System Action: Processing for the ADDVOL or ALTVOL operand stops.

ICH22010I VOLUME SPECIFIED DOES NOT EXIST IN DATASET PROFILE

Explanation: The DELVOL or ALTVOL operand was specified which requests a volume to be deleted from the data set profile but the volume does not exist in the profile.

System Action: Processing for the DELVOL or ALTVOL operand stops.

ICH22011I VOLUME SPECIFIED IS LAST VOLUME IN DATASET PROFILE. NO CHANGE MADE

Explanation: The DELVOL operand was specified which requested that the last volume be deleted from the data set profile. This is not a valid request for the ALTDSD command.

System Action: Processing for the DELVOL operand stops.

ICH22012I NOT AUTHORIZED TO SPECIFY NOSET/ALTVOL

Explanation: You do not have sufficient authority to specify the NOSET or ALTVOL operand.

System Action: The NOSET, ADDVOL, ALTVOL, and DELVOL operands are ignored.

User Response: See your RACF security administrator.

ICH22013I ADDVOL/DELVOL NOT PROCESSED

Explanation: While adding or deleting a volume, the command processor could not establish the required ESTAE recovery environment. Other operands have already been processed.

User Response: Report this message to your system programmer. Please include the following:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH22014I NOT AUTHORIZED TO SPECIFY GLOBALAUDIT FOR *profile-name*; OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the GLOBALAUDIT operand for the indicated profile name.

System Action: RACF ignores the operand for the indicated profile name.

User Response: See your RACF security administrator.

ICH22015I AUTHORIZED TO ISSUE ONLY GLOBALAUDIT FOR *profile-name*; REMAINING OPERANDS IGNORED

Explanation: You do not have sufficient authority to specify any operand except GLOBALAUDIT for the indicated profile name.

System Action: RACF ignores all other operands for the indicated profile name.

User Response: See your RACF security administrator.

ICH22016I VOLUME SPECIFIED ALREADY EXISTS IN ANOTHER PROFILE FOR SAME DATA SET NAME

Explanation: An ADDVOL or ALTVOL request was specified, but the volume serial number to be added to the data set profile specified is already defined in another data set profile of the same name.

System Action: The volume serial number is not added.

ICH22017I ALTVOL PROCESSING ENDED DUE TO ERROR

Explanation: While processing the ALTVOL operand, the command processor encountered an error that caused processing to stop. Other operands have already been processed.

ICH22018I INSTALLATION EXIT FAILED ALTER REQUEST FOR *profile-name*

Explanation: The command preprocessing exit routine ICHCNX00 issued a return code of 4, indicating that RACF should fail the ALTDSD request for the profile name indicated in the message.

System Action: Command processing stops.

User Response: Report this message to your system programmer.

ICH22020I • ICH22028I

ICH22020I **GENERIC INVALID, GENERIC COMMAND PROCESSING NOT ACTIVE**

Explanation: Because the generic command processing facility is inactive, the GENERIC operand is not valid.

System Action: Command processing stops.

ICH22021I *category* **ALREADY DEFINED TO profile-name.**

Explanation: The specified category has already been defined in this profile.

System Action: RACF ignores the category. Command processing continues with the next operand.

ICH22022I *category* **NOT DEFINED TO** *profile-name.*

Explanation: The specified category has not been defined in this profile; therefore, deletion is impossible.

System Action: RACF ignores the category. Command processing continues with the next operand.

ICH22023I **'NOTIFY IGNORED' SPECIFIED USER IS NOT DEFINED TO RACF**

Explanation: The user ID specified for the NOTIFY operand is not a RACF-defined user ID.

System Action: Command processing continues with the next operand.

ICH22024I **NOT AUTHORIZED TO USE VOLUME** *volume*

Explanation: You do not have allocation authority to the volume specified.

System Action: Command processing stops.

User Response: See your RACF security administrator.

ICH22025I **UNABLE TO LOCATE TAPE VOLUME FOR TAPE DATA SET** *dsname*

Explanation: The tape volume profile named in the indicated tape data set profile could not be located. This error indicates a problem with the RACF database.

System Action: Command processing continues with the next data set.

User Response: See your RACF security administrator.

Problem Determination: Do the following:

1. Use the LISTDSD command to display profile *dsname*. In the LISTDSD output, check the VOLUME ON WHICH DATASET RESIDES and UNIT fields for a possible error.

2. If no error is apparent in the LISTDSD output, use the RLIST command to display the profile named in the VOLUME ON WHICH DATASET RESIDES field. Check the output of the RLIST command for a possible error.

ICH22026I **UNABLE TO LOCATE TAPE VOLUME ENTRY FOR TAPE DATA SET** *dsname*

Explanation: A TVTOC entry could not be located after a discrete profile for the tape data set indicated by *dsname* was found. RACF searched for a TVTOC entry in one of the following places:

- The TVTOC of the volume specified in the ADDVOL or DELVOL operand of the ALTDSD command
- The TVTOC of the volume specified in the data set profile, if ADDVOL and DELVOL were not specified on the ALTDSD command and this is a tape data set.

System Action: Command processing continues with the next data set.

User Response: Do one of the following:

- If ADDVOL or DELVOL was specified on the ALTDSD command, check the spelling of the volume specified on the ADDVOL or DELVOL operands. If the spelling is correct, check that the volume specified actually contains part of the data set specified.
- If ADDVOL and DELVOL were not specified on the ALTDSD command, do the following:
 1. Use the LISTDSD command to display profile *dsname*. In the LISTDSD output, check the VOLUME ON WHICH DATASET RESIDES and UNIT fields for a possible error.
 2. If no error is apparent in the LISTDSD output, use the RLIST command to display the profile named in the VOLUME ON WHICH DATASET RESIDES field. Check the output of the RLIST command for a possible error.

ICH22027I **ALTVOL OPERAND INCONSISTENT WITH TAPE DS PROFILE FOR DATA SET** *profile-name.*

Explanation: A tape data set profile was found when an ALTVOL request was entered. RACF does not support ALTVOL processing for tape data sets.

System Action: ALTVOL processing continues with the next profile specified on the ALTDSD command.

ICH22028I **TAPE DATA SET SPECIFIED NOT LAST ON VOLUME - ADDVOL/DELVOL IGNORED**

Explanation: The ADDVOL or DELVOL operand was entered for a tape data set that is not the last one on the tape volume set.

System Action: RACF ignores the operand.

Command processing continues with the next data set name.

**ICH22029I TVTOC UPDATE FAILED.
ADDVOL/DELVOL BYPASSED FOR
DATA SET PROFILE *dsname***

Explanation: When ADDVOL or DELVOL operand processing attempted to update the tape data set entry in the TVTOC of the TAPEVOL profile, a RACF-manager error occurred.

System Action: RACF does not update the TVTOC. Command processing continues with the next data set name.

**ICH22030I VOLSER LIST INCONSISTENT WITH
ADDVOL/DELVOL OPERAND FOR
TAPE DS *dsname***

Explanation: For ADDVOL, the VOLSER specified in the command was found in the tape volume list. For DELVOL, the VOLSER specified in the command was not found in the list.

System Action: The ADDVOL/DELVOL operand for this data set is bypassed. Command processing continues with the next data set name.

**ICH22031I COMMAND PROCESSING
TERMINATED. NO {SECLEVELS |
CATEGORIES} FOUND**

Explanation: RACF could not validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System Action: Command processing stops.

**ICH22032I NOT AUTHORIZED TO DFP SEGMENT
FOR DATASET PROFILE *profile-name*
DATASET PROFILE NOT PROCESSED**

Explanation: You specified the RESOWNER operand on the ALTDSD command, but you are not authorized to the DFP segment for the specified data set profile.

System Action: Command processing stops with no update to the data set profile.

User Response: See your RACF security administrator for authority to the DFP segment of this profile.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

ICH22033I DFP OPERAND NOT PROCESSED

Explanation: You are not authorized to alter the RESOWNER field of the specified data set profile.

System Action: Command processing stops.

User Response: See your RACF security administrator for authority to this segment.

**ICH22034I ALTDSD failed. You are not authorized
to specify SECLABEL or
NOSECLABEL.**

Explanation: The SECLABEL operand was specified on the ALTDSD command and one of the following conditions is true:

- The user did not have the SPECIAL attribute and SETROPTS SECLABELCONTROL was in effect.
- SETROPTS MLSTABLE was in effect, but SETROPTS MLQUIET was not in effect.

System Action: Command processing stops.

User Response: See your RACF security administrator.

**ICH22035I ALTDSD failed. SECLABEL
seclabel-name is not currently defined
to RACF.**

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System Action: Command processing stops.

User Response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, report the exact text of this message to your RACF security administrator.

**ICH22036I ALTDSD failed. NOSECLABEL is not
allowed under the current RACF
options.**

Explanation: The NOSECLABEL operand was specified on the ALTDSD command. You cannot do this when SETROPTS MLACTIVE is on.

System Action: Command processing stops.

User Response: Correct the command.

**ICH22037I ALTDSD failed. You are not authorized
to specify SECLABEL *seclabel-name*.**

Explanation: To specify the security label indicated in the message, you must have at least READ access authority to the SECLABEL profile indicated in the message.

System Action: Command processing stops.

User Response: See your RACF security administrator.

LISTUSER command messages

ICH30001I UNABLE TO LOCATE {USER | GROUP | CONNECT} ENTRY *profile-name*

Explanation: The indicated profile name could not be found on the RACF database.

System Action: If a user profile cannot be located, processing continues with the next profile. If a group or connect profile cannot be located, then an inconsistency exists on the RACF database.

Problem Determination: The RACF utility programs may be needed to determine the inconsistency. All information that is available is listed.

ICH30002I NOT AUTHORIZED TO LIST {*userid*, *}

Explanation: You do not have sufficient authority to list the indicated user ID or to specify *.

System Action: Command processing stops.

User Response: If you are attempting to list your own user ID, enter the LISTUSER command without operands. Otherwise, see your RACF security administrator.

ICH30003I GROUP *group-name* USER CONNECTION NOT INDICATED

Explanation: The user profile being listed identifies the indicated group as a connected group, but the group profile does not reference the user. An inconsistency exists on the RACF database.

Problem Determination: The RACF utility programs may be needed to determine the inconsistency. All information that is available is listed.

ICH30010I NOT AUTHORIZED TO ISSUE LISTUSER

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security*

Server RACF Command Language Reference.

ICH30011I NO USERS LISTED.

Explanation:

- You issued LISTUSER *, but you are not authorized to list any users,
or
- You issued LISTUSER * *segment-name* NORACF, and no users with the specified segment were found.

ICH30012I NO USER(S) LISTED. NORACF SPECIFIED AND NO OTHER SEGMENTS REQUESTED.

Explanation: RACF cannot list users when NORACF is specified. Listing users for other segments has not been requested.

System Action: Command processing stops with no output produced.

User Response: If you specify NORACF, you must specify an operand that requests output, such as DFP, TSO/E, or DSNS.

ICH30014I LISTUSER failed. Parameter list error detected while translating a SECLABEL.

Explanation: An internal RACF error has been detected.

System Action: Command processing stops.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

ICH30015I This SECLABEL is not currently defined to RACF.

Explanation: The security label specified in the user profile does not exist as a profile in the SECLABEL class.

System Action: Command processing continues without listing the description of the security label.

User Response: Report this message to your RACF security administrator.

SEARCH command messages

ICH31001I NOT AUTHORIZED TO ISSUE *command-name*

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH31002I UNABLE TO OPEN CLIST DATASET, COMMAND TERMINATED

Explanation: SEARCH command processing SEARCH could not open the specified CLIST data set.

System Action: Command processing stops.

ICH31003I MASK TOO LONG, COMMAND TERMINATED

Explanation: The character string specified on the MASK operand is longer than the maximum allowable length for the profile name in the specified class. For the DATASET class, the maximum length is 44 characters; for the DASDVOL and TAPEVOL classes, the maximum length is 6 characters; and for the TERMINAL class, the maximum length is 8 characters.

System Action: Command processing stops.

ICH31004I LIST AND CLIST OMITTED, COMMAND TERMINATED

Explanation: CLIST must be specified on the SEARCH command when NOLIST is specified.

System Action: Command processing stops.

ICH31005I NO ENTRIES MEET SEARCH CRITERIA

Explanation: One or more of the following occurred:

- There are no RACF profiles that meet the search criteria.

- You do not have sufficient authority to list the profiles that match the search criteria.

ICH31006I CLIST DATA SET ORGANIZATION IS NOT SEQUENTIAL OR PARTITIONED. COMMAND TERMINATED.

Explanation: The CLIST data set for the SEARCH command must have either the physical sequential (PS) organization or the partitioned organization (PO). The CLIST data set found does not have one of these organizations.

User Response: See your system programmer.

System Programmer Response: Make sure the CLIST data set, *userid.EXEC.RACF.CLIST*, is either a partitioned data set or a sequential data set.

System Action: Command processing stops.

ICH31007I COMMAND ENDED DUE TO ERROR

Explanation: A RACF manager error occurred. This message is accompanied by a message explaining the error.

ICH31008I CATEGORY *category-name* IGNORED

Explanation: The user does not have sufficient authority to list the entries in the RACF data set for the security category name specified on the command, or the security category name does not exist.

User Response: See your RACF security administrator.

ICH31009I FILTER STRING LONGER THAN PROFILE NAMES

Explanation: A filter string was specified longer than the maximum allowable for a profile name in that class.

System Action: Command processing stops.

ICH31010I FILTER AND MASK BOTH SPECIFIED

Explanation: The FILTER operand is an alternative to the MASK operand; they are mutually exclusive.

System Action: Command processing stops.

ICH31011I BLANK FOUND IN FILTER STRING

Explanation: The filter string cannot contain blanks.

System Action: Command processing stops.

ICH31012I CHARACTER FOUND AFTER ** IN FILTER STRING

Explanation: Double asterisks must be the last (rightmost) characters in the filter string.

System Action: Command processing stops.

ICH31013I INVALID LEADING CHARACTER IN FILTER STRING

Explanation: A character that is not allowed was used to start a filter string.

System Action: Command processing stops.

ICH31014I INVALID USE OF ** IN FILTER STRING

Explanation: Double asterisks cannot be mixed with other characters within a qualifier.

System Action: Command processing stops.

ICH31015I INVALID USE OF * IN FILTER STRING

Explanation: The asterisk is used incorrectly.

System Action: Command processing stops.

ICH31016I INVALID CHARACTER IN FILTER STRING

Explanation: A character(s) that is not considered valid was specified in a filter string. Only alphanumeric characters, a single asterisk (*), a double asterisk (**), or the percent sign (%) are allowed.

System Action: Command processing stops.

ICH31017I FILTER QUALIFIER LENGTH INVALID FOR CLASS

Explanation: The specified filter string is too long. The filter string length must not exceed 44 characters for a tape or DASD data set name. For general resource classes, the filter string must not exceed the length specified in the class descriptor table.

System Action: Command processing stops.

ICH31018I INVALID FILTER STRING

Explanation: An error was detected in the specified filter string.

System Action: Command processing stops.

ICH31021I NOT AUTHORIZED TO SPECIFY USER *userid*

Explanation: You are not authorized to list information about the user specified by the USER operand.

System Action: Command processing stops.

ICH31022I USER *userid* IS NOT DEFINED TO RACF

Explanation: The user specified by the USER operand is not defined to RACF.

System Action: Command processing stops.

ICH31023I RACINIT WAS FAILED BY THE INSTALLATION EXIT ROUTINE

Explanation: RACROUTE REQUEST=VERIFY processing for the user specified by the USER operand was failed by the installation exit routine.

System Action: Command processing stops.

ICH31024I THE ACCESS OF THE SPECIFIED USER HAS BEEN REVOKED

Explanation: RACROUTE REQUEST=VERIFY processing for the user specified by the USER operand failed because the access of the user has been revoked.

System Action: Command processing stops.

ICH31025I USER ACCESS TO THE DEFAULT GROUP HAS BEEN REVOKED

Explanation: RACROUTE REQUEST=VERIFY processing for the USER specified by the USER operand failed because this user's access to the default group has been revoked.

System Action: Command processing stops.

ICH31026I UNEXPECTED RETURN CODE *return-code* FROM RACINIT

Explanation: RACROUTE REQUEST=VERIFY processing for the user specified by the USER operand failed with an unexpected return code.

System Action: Command processing stops.

ICH31027I *command-name* failed. SECLABEL *seclabel-name* is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System Action: Command processing stops.

User Response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, report the exact text of this message to your RACF security administrator.

ICH31028I

ICH31028I The [UID|GID] keyword requires application identity mapping to be implemented.

Explanation: The UID or GID keyword has been specified on the SEARCH command, but the RACF database has not been converted to the use of application identity mapping. Application identity mapping must be enabled in order for SEARCH to be able to map UIDs and GIDs to USER and GROUP profiles. Use of the UNIXMAP class is not sufficient. The RACF database must be at least at stage 2 of application identity mapping.

System Action: Command processing stops.

System Programmer Response: Use the IRRIRA00 utility to convert the RACF database to at least stage 2 of application identity mapping. See the *z/OS Security Server RACF System Programmer's Guide* for information about the IRRIRA00 utility. Once this is complete, the user may reissue the command.

User Response: Contact your system programmer.

LISTGRP command messages

ICH32002I NOT AUTHORIZED TO LIST BASE INFORMATION FOR GROUP *group-name*

Explanation: You do not have sufficient authority to list the group profile indicated in the message.

System Action: Command processing continues with the next group specified.

User Response: See your RACF security administrator.

ICH32004I NOT AUTHORIZED TO ISSUE LISTGRP

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH32005I NO GROUPS LISTED

Explanation:

- You issued LISTGRP *, but are not authorized to list any groups,
or
- You issued LISTGRP * *segment-name* NORACF, and no groups with the specified segment were found.

User Response: See your RACF security administrator.

ICH32006I NOT AUTHORIZED TO DISPLAY DFP SEGMENT IN GROUP PROFILE *group-name*

Explanation: You are not authorized to display a DFP segment.

System Action: Command processing stops.

User Response: See your RACF security administrator for authority to this segment.

RACF Security Administrator Response: See the command description in *z/OS Security Server RACF Command Language Reference* for the authority required to list the indicated segment.

ICH32007I NO SEGMENT REQUESTED

Explanation: You specified NORACF (which requests no display for the RACF segment of a group profile), but did not specify any other segment (such as DFP).

System Action: Command processing continues with no segment displayed.

User Response: Either specify another segment to be displayed or omit the NORACF operand. Enter the command again.

LISTDSD command messages

ICH35001I COMMAND ENDED DUE TO ERROR

Explanation: A RACF-manager error occurred. This message is accompanied by a message explaining the error.

ICH35002I NOT AUTHORIZED TO LIST *profile-name*

Explanation: You do not have sufficient authority to the profile indicated in the message and cannot list the profile.

System Action: Command processing continues with the next profile.

User Response: See your RACF security administrator.

ICH35003I NO RACF DESCRIPTION FOUND FOR *dsname*

Explanation: No profile could be found in the RACF database for the data set indicated in the message for one of the following reasons:

- The data set profile does not exist.
- The data set profile requested is a fully qualified generic, and the GENERIC operand was not specified in the command string.
- The data set profile requested is discrete, the GENERIC operand was specified, and there is no generic profile that closely matches the discrete profile name.

User Response: If the LISTDSD command was issued without the GENERIC operand, and this data set profile is generic, issue the command again with the GENERIC operand. If the LISTDSD command was issued with the GENERIC operand, and this data set profile is discrete, issue the command again without the GENERIC operand.

ICH35004I NOT AUTHORIZED TO ISSUE LISTDSD

Explanation: One of the following is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System Action: Command processing stops.

User Response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient

authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see *z/OS Security Server RACF Command Language Reference*.

ICH35005I NO DATASETS LISTED

Explanation: No data sets were found that you are authorized to list.

ICH35006I INSTALLATION EXIT FAILED LIST REQUEST FOR *profile-name*

Explanation: The command preprocessing exit routine ICHCNX00 issued a return code of 4, indicating that RACF should fail the LISTDSD request for the indicated profile.

System Action: Processing of the LISTDSD command continues with the next profile specified.

User Response: Report this message to your system programmer.

ICH35007I NO RACF DESCRIPTION FOUND ON THE SPECIFIED VOLUME(S) FOR *dsname*

Explanation: The RACF database does not contain a discrete profile for the indicated data set for any of the volume serials given in the LISTDSD command.

ICH35009I NOT AUTHORIZED TO LIST DFP SEGMENT FOR DATASET PROFILE *dsname*

Explanation: The RESOWNER operand was specified for the LISTDSD command, but you are not authorized to display the DFP segment for a data set profile.

System Action: Command processing stops.

User Response: See your RACF security administrator for authority to this segment.

RACF Security Administrator Response: See the command description in *z/OS Security Server RACF Command Language Reference* for the authority required to list the indicated segment.

ICH35010I No profile(s) listed. NORACF specified and no other information requested.

Explanation: You specified NORACF (which requests no display for the RACF segment of a data set profile), but did not request any other output (such as another segment like the DFP segment or the DSNS operand).

System Action: Command processing continues with no segment displayed.

User Response: Either specify other output to be listed (such as the DFP or DSNS operand) or omit the NORACF operand. Enter the command again.

ICH35011I LISTDSD failed. Error encountered during catalog processing.

Explanation: LISTDSD DSNS was issued, but there are no cataloged data sets that are protected by the specified profile.

System Action: The command executes but no data set names are displayed.

ICH35012I LISTDSD cannot obtain this data in an MVS/370 environment.

Explanation: LISTDSD DSNS was issued from an MVS/370 environment. The DSNS operand is not supported in an MVS/370 environment.

System Action: The command executes but no data set names are displayed.

Chapter 3. Miscellaneous RACF ICH messages

This section lists the messages issued by:

- RACF command processors, when the messages reflect errors in the RACF manager
- RACF report writer
- Data security monitor

RACF routes these messages to the user.

The format of these messages is:

ICHxxnnnt text

where:

ICH identifies the message as a RACF message.
xx identifies the function issuing the message.
nnn is the message serial number.
t is the type code (I = information, or A = action).
text is the text of the message.

The values for the *xx* field that identifies the function issuing the message are:

xx	Function/Program
51	RACF manager (see “Note”)
64	RACF report writer (RACFRW)
66	Data security monitor (DSMON)
70	Miscellaneous

Note: These common error messages are issued by the various RACF command processors based on return codes from the RACF manager.

RACF manager error messages

ICH51001I SVC 132 UNABLE TO INVOKE PROCESSING ROUTINE

Explanation: RACF was unable to invoke the appropriate processing routine (RACF manager, RACROUTE REQUEST=LIST) because of one of the following errors, whose code is returned in register 0:

Code	Description
0	Unable to establish ESTAE environment.
1	The function code (third byte of parameter list) does not represent a valid function.

ICH51002I NAME TO BE ADDED TO RACF DATA SET ALREADY EXISTS

Explanation: The user or group name that was requested to be added to the RACF database already exists on the RACF database; for example, if you

attempted to add user X, and group X already exists.

ICH51003I NAME NOT FOUND IN RACF DATA SET

Explanation: A profile requested by the command does not exist on the RACF database. If the command does not issue a message giving the profile name, the RACF list commands (LISTDSD, LISTGRP, and LISTUSER) can be used to determine inconsistencies in profiles associated with the command.

ICH51004I PARAMETER LIST ERROR DETECTED BY RACF MANAGER

Explanation: The RACF manager has detected one of the following errors:

- Input parameter list error. The following codes are returned in register 0:

Code	Description
------	-------------

ICH51005I • ICH51012I

- 1 Entry name (profile name) incorrect
- 2 Action specified for delete
- 3 Incorrect field name
- 4 Test specified for rename request
- 7 Entry type (profile type) incorrect.

- User work area not large enough to hold all the data.
- User work area smaller than minimum allowable size.

ICH51005I ATTEMPT TO DELETE RESTRICTED NAME DENIED BY RACF MANAGER

Explanation: An attempt was made to delete a restricted name.

ICH51006I ALTER IN PLACE REQUEST REJECTED BY RACF MANAGER

Explanation: The requested ALTERI operation is invalid.

ICH51007I RACF DATABASE CANNOT BE ALTERED.

Explanation: The RACF database cannot be altered for one or more of the following reasons:

- The database has been locked by a RACF utility.
- The system that attempted to alter the database is currently in read-only mode (in a RACF sysplex data sharing environment).

ICH51008I DUPLICATE DATASET NAME FOUND BUT VOLUME NOT SPECIFIED

Explanation: In processing a data set request, the RACF manager found duplicate data set profiles in the RACF database and did not process the request because the VOLUME operand was not specified on the request.

ICH51009I VOLUME NOT FOUND

Explanation: In processing a data set request, the RACF manager searched all the data set profiles that have the name specified in the command. However, the RACF manager could not find the volume serial number that you specified in any of those profiles.

ICH51010I RACF DATASET ACCESS DENIED—RACF IS NOT ACTIVE OR THE RACF DATASET CONTAINING THE REQUESTED PROFILE NOT ACTIVE

Explanation: The RACF manager could not complete the requested operation because RACF is currently not active.

ICH51011I RACF MANAGER PROCESSING ENDED DUE TO ERROR. RETURN CODE = *return-code*

Explanation: The RACF manager could not complete the requested operation because of a system error or a problem with the RACF database. The return code, which is displayed in decimal format, is a RACF manager return code that is not recognized by the command processor that invoked the RACF manager.

Problem Determination: If there is an error in the RACF database, the RACF manager issues message ICH411I preceding this message. See this message for information on how to resolve the problem.

Note: If the user is not receiving write-to-programmer messages, message ICH411I cannot be received. To receive this message, issue the TSO/E command PROFILE WTPMSG MSGID and rerun the RACF command or utility.

Check the list of RACF-manager return codes in “RACF Manager Return Codes” on page 307. If the return code is listed, the explanation should help you investigate the problem. If the return code is not listed or relates to a problem with RACF (as opposed to a problem you can fix in the RACF database), report the complete text of this message to your IBM support center.

For certain return codes, this message might be issued because there is a bad profile in the RACF database. To find the bad profile, enter the SEARCH command. With a bad profile in the database, this command is likely to fail also. The profile after the last one listed is probably the bad profile. Because this command might take a long time to run and might produce many lines of output, you might wish to execute the command in batch.

ICH51012I RACF AUTHORITY DENIED BY FIELD LEVEL ACCESS CHECKING

Explanation: You do not have sufficient authority for access at the field level. The RACF database is not updated.

User Response: See your RACF security administrator.

RACF Report Writer (RACFRW) messages

ICH64001I **SUBCOMMAND** *subcommand-name*
NOT FOUND+ ANY SUBCOMMAND
ENTERED AFTER *subcommand-name*
MUST BE REENTERED

Explanation: The RACF report writer does not support the subcommand name entered.

System Action: The RACF report writer ignores this subcommand and all subsequent RACF report writer subcommands. The RACF report writer prompts the user to enter another subcommand.

User Response: The user must enter another subcommand. For more information, see the *z/OS Security Server RACF Auditor's Guide*.

ICH64002I **TOO MANY SUBCOMMANDS; IMAGES**
LOST ON OUTPUT LISTING

Explanation: The user has entered more than the maximum number (100) of subcommands that the RACF report writer can reproduce on the output listing.

System Action: Although all the subcommands are processed, the list of subcommands appearing on the output listing is incomplete. The RACF report writer prompts the user to enter another subcommand.

User Response: The user must enter another subcommand. For more information, see *z/OS Security Server RACF Auditor's Guide*.

ICH64003I *report-name* **REPORT COMPLETE**

Explanation: The named report has been completed successfully.

System Action: The RACF report writer continues with the next report or, if all reports have been processed, ends normally.

ICH64004I *operand* **DOES NOT APPLY TO STATUS**
RECORDS; OPERAND IGNORED

Explanation: On the SELECT subcommand, the user has specified the named operand along with the STATUS operand.

System Action: Because the named operand has no meaning for status records, the RACF report writer ignores it. The RACF report writer prompts the user to enter another subcommand.

User Response: The user must enter another subcommand. For more information, see *z/OS Security Server RACF Auditor's Guide*.

ICH64005I **LIMIT OF 50 SELECT AND EVENT**
SUBCOMMANDS HAS BEEN
EXCEEDED; *subcommand-name*
IGNORED

Explanation: The user has entered more than the maximum number (50) of SELECT and EVENT subcommands.

System Action: The RACF report writer ignores the subcommand. The RACF report writer prompts the user to enter a subcommand other than SELECT or EVENT.

User Response: The user must enter another subcommand. For more information, see *z/OS Security Server RACF Auditor's Guide*.

ICH64006I **OPERAND DOES NOT APPLY TO**
event-name **EVENT; OPERAND**
IGNORED

Explanation: On the EVENT subcommand, the user specified an operand that is not valid for the named event.

System Action: The RACF report writer ignores the operand. The RACF report writer prompts the user to enter another subcommand.

User Response: The user must enter another subcommand. For more information, see *z/OS Security Server RACF Auditor's Guide*.

ICH64007I **THERE IS NO PRECEDING SELECT**
SUBCOMMAND FOR THIS EVENT
SUBCOMMAND; EVENT IGNORED

Explanation: The user has entered an EVENT subcommand without first having entered any SELECT subcommands.

System Action: The RACF report writer ignores the EVENT subcommand. The RACF report writer prompts the user to enter another subcommand.

User Response: The user must enter another subcommand. For more information, see *z/OS Security Server RACF Auditor's Guide*.

ICH64008I **INVALID SUBCOMMAND**

Explanation: The user has entered a subcommand that violates the syntax rules for subcommand names.

System Action: The RACF report writer ignores the subcommand. The RACF report writer prompts the user to enter another subcommand.

User Response: The user must enter another subcommand. For more information, see *z/OS Security Server RACF Auditor's Guide*.

**ICH64009I NOUSER/NOJOB COMBINATION
INVALID; BOTH OPERANDS IGNORED**

Explanation: On the SELECT subcommand, the user has specified both the NOUSER and the NOJOB operands.

System Action: The RACF report writer ignores both operands and uses the defaults (USER and JOB) to select all user IDs and job names.

User Response: Enter next subcommand.

**ICH64301I RACFRW ENDED DUE TO PUTGET
ERROR + PUTGET RETURN CODE**
return-code

Explanation: While the RACF report writer was prompting the user to enter a subcommand, an error occurred in the PUTGET TSO/E service routine.

System Action: The RACF report writer stops.

User Response: See your system programmer.

System Programmer Response: For an explanation of the TSO/E service routines return codes, see *z/OS TSO/E Programming Services*. For the order number of the documentation you need, see *z/OS TSO/E General Information*.

**ICH64302I RACFRW ENDED DUE TO IKJSCAN
ERROR + IKJSCAN RETURN CODE**
return-code

Explanation: An error occurred in the IKJSCAN TSO/E service routine while it was checking the syntax of a RACFRW subcommand.

System Action: The RACF report writer stops.

User Response: See your system programmer.

System Programmer Response: For an explanation of the TSO/E service routines return codes, see *z/OS TSO/E Programming Services*. For the order number of the documentation you need, see *z/OS TSO/E General Information*.

ICH64303I FILE *ddname* COULD NOT BE OPENED

Explanation: The RACF report writer could not open the file identified by *ddname*.

System Action: The RACF report writer stops.

User Response: Ensure that the DD statement exists or that the data set has been preallocated.

**ICH64304I SORT ERROR RETURN CODE
'*return-code*' OCCURRED WHILE
PRODUCING '*report-name*' REPORT;
COMMAND TERMINATED**

Explanation: The sort function invoked by RACF (DFSORT) encountered an error while sorting the records for the named report.

System Action: The RACF report writer stops.

User Response: See your system programmer.

System Programmer Response: Check for an error in module ICHRSMFI, which is an installation-replaceable module used by the RACF report writer. For an explanation of the sort return codes, see *DFSORT Messages, Codes and Diagnosis Guide R14*.

**ICH64305I NO INPUT DATASET ALLOCATED;
COMMAND TERMINATED**

Explanation: The user did not preallocate the RSMFIN file or did not specify the DATASET operand on the RACFRW command.

System Action: The RACF report writer stops.

User Response: Preallocate the file RSMFIN or specify the DATASET operand on the RACFRW command. For more information, see the *z/OS Security Server RACF Auditor's Guide*.

Data Security Monitor (DSMON) messages

ICH66001I ICHDSM00 STARTED ON *mm/dd/yy* AT *hh:mm:ss*

Explanation: Data security monitor execution began at this date and time.

ICH66002I FUNCTION *name* ENDED SUCCESSFULLY

Explanation: The data security monitor performed the specified test function.

System Action: Processing continues with the next function.

Note: For an explanation of the test functions that the data security monitor performs, see the *z/OS Security Server RACF Auditor's Guide*.

ICH66003I ICHDSM00 ENDED ON *mm/dd/yy* AT *hh:mm:ss* - RETURN CODE = *nn*

Explanation: Data security monitor execution stops at this date and time with the specified return code. The return codes that can appear in this message are:

Code	Description
0	The data security monitor completed execution successfully.
16	The execution of one or more test functions was unsuccessful.
20	An attempt to open the data set specified in message ICH66101I failed.

ICH66004I USER NOT AUTHORIZED TO EXECUTE THE DATA SECURITY MONITOR - RETURN CODE = 16

Explanation: DSMON is not a controlled program, but you cannot execute the DSMON program because you do not have the system AUDITOR attribute.

System Action: The program ends with return code 16 and produces no reports.

Note: Because the SYSPRINT data set is not opened unless the user is authorized to execute the data security monitor, the data security monitor issues this message to the programmer's console with a write-to-operator instruction (routing code 11) and to the system security console (routing code 9).

User Response: See your RACF security administrator.

ICH66009I ---START OF INPUT LISTING---

Explanation: The data security monitor has started to read the input control statements from the SYSIN data set. A listing of each control statement follows this message.

ICH66010I ---END OF INPUT LISTING---

Explanation: The data security monitor has finished reading the input control statements from the SYSIN data set.

ICH66011I ABOVE CONTROL CARD IGNORED. UNKNOWN TYPE

Explanation: The control statement that precedes the message did not have a valid control statement identifier (FUNCTION, USEROPT, or LINECOUNT) and was not a continuation of the prior statement.

System Action: Processing continues with the next control statement.

ICH66012I ERROR IN ABOVE CONTROL CARD. *xxxxxxx* IS AN UNKNOWN FUNCTION TYPE AND IS IGNORED

Explanation: The FUNCTION statement that precedes the message includes an invalid function name.

System Action: Processing continues with the next control statement.

ICH66013I ABOVE CONTROL CARD IGNORED. *xxxxxxx* IS AN UNKNOWN USEROPT TYPE

Explanation: The USEROPT statement that precedes the message includes an invalid function name.

System Action: Processing continues with the next control statement.

ICH66014I ABOVE CONTROL CARD IGNORED. INCORRECT LINECOUNT VALUE

Explanation: The lines per page indicated by the LINECOUNT statement was too great, too small, or non-numeric.

System Action: Processing continues with the next control statement.

ICH66015I EXTRANEIOUS INFORMATION IGNORED IN ABOVE CONTROL CARD

Explanation: The LINECOUNT statement contained extra information after the lines per page information.

ICH66016I • ICH66102I

System Action: Processing continues with the next control statement.

**ICH66016I NO xxxxxx FUNCTION CARD FOUND.
ANY RELATED USEROPT
STATEMENTS WILL BE IGNORED**

Explanation: DSMON found a USEROPT statement for function xxxxxx, but there is no matching FUNCTION statement.

System Action: Processing continues with the next control statement.

**ICH66017I ABOVE CONTROL CARD IGNORED.
NO FUNCTION SPECIFIED**

Explanation: DSMON found a function card with no functions specified.

System Action: Processing continues with the next control statement.

**ICH66018I ABOVE CONTROL CARD IGNORED.
INCOMPLETE SPECIFICATION**

Explanation: DSMON found a USEROPT statement with no user value specified. Processing continues with the next control statement.

ICH66019I ERROR IN ABOVE CONTROL CARD

Explanation: DSMON found incorrect data on a control statement. Message ICH66020I follows this message.

ICH66020I FOLLOWING INPUT DATA IGNORED:...

Explanation: The indicated input data is incorrect. DSMON ignores it.

System Action: Processing continues with the next control statement.

**ICH66021I EXPECTED CONTROL CARD
CONTINUATION NOT FOUND**

Explanation: The previous input control statement contained a continuation character, indicating that another control statement involving the same statement would follow. DSMON did not find that control statement.

System Action: Processing continues with the next control statement.

ICH66101I OPEN FAILED FOR DDNAME *name*

Explanation: An error occurred during the OPEN issued for the named data set. If the data set that cannot be opened is SYSPRINT, RACF issues this message to the programmer's console with a

write-to-operator message (routing code 11).

User Response: See your system programmer.

**ICH66102I FUNCTION *name* ENDED
UNSUCCESSFULLY - ERROR CODE =
*nnn***

Explanation: The specified test function ended abnormally with the specified error code. This is a right-justified integer code which can range from 1 to 999.

System Action: Processing continues with the next function.

User Response: See your system programmer.

Problem Determination: The following table contains a list of the test functions and their associated error codes:

Function	Code	Description
LNKLST	3	An error occurred while attempting to retrieve LNKLST libraries.
SYSAPF	1	There were no entries in the list of APF libraries.
SYSLNK	1	An error occurred while attempting to open the SYS1.PARMLIB data set.
SYSLNK	2	An error occurred while attempting to open SYSUT1.
SYSPPT	1	RACF could not locate the program properties table (PPT).
SYSPPT	2	An error occurred while attempting to load module IEFSD060, which contains the program properties table (PPT).
RACUSR	1	An error occurred while attempting to access a user profile in the RACF database.
RACUSR	2	An error occurred while attempting to access a group profile in the RACF database.
RACEXT	1	Either the entry point address of the specified RACF exit did not correspond with the address contained in the RACF communications vector table (RCVT), or an error occurred while attempting to load a RACF exit routine module defined by the installation.
RACGRP	1	An error occurred while attempting to access a group profile in the RACF database.
RACGAC	1	There are no classes eligible for global access checking.

Note: Functions not named in the preceding list have no associated error codes.

ICH66103I RACF IS INACTIVE OR VERSION IS INVALID - ONLY SYSTEM REPORT PRODUCED

Explanation: One of the following conditions occurred: (1) RACF is not installed; (2) RACF is inactive; or (3) the RACF version that is active is prior to RACF Version 1 Release 6.

System Action: The data security monitor produces the system report and ends.

User Response: See your system programmer.

ICH66104I PROGRAM PROPERTIES TABLE NOT FOUND

Explanation: The data security monitor could not locate the program properties table; therefore, the data security monitor does not produce the program properties table report.

System Action: Processing continues with the next function.

User Response: See your system programmer.

ICH66105I RACF MANAGER ERROR - RETURN CODE = *return-code*

Explanation: The RACF manager encountered an error while attempting to retrieve RACF user attributes, as indicated by the return code in the message.

System Action: Processing continues with the next function.

User Response: See your system programmer.

Problem Determination: For a description of the return codes see "RACF Manager Return Codes" on page 307.

ICH66106I ERROR OCCURRED DURING MEMBERLIST RETRIEVAL

Explanation: The data security monitor encountered an error while attempting to retrieve a list of partitioned data set (PDS) members.

System Action: Processing continues with the next function.

User Response: See your system programmer.

ICH66107I EXIT *name* HAS INVALID RCVT ADDRESS

Explanation: The entry point address of the named RACF exit routine does not correspond with the address contained in the RACF communications vector table

(RCVT). This difference might indicate a system integrity exposure.

User Response: Report the exact text of this message to your system programmer.

ICH66108I ERROR OCCURRED WHILE LOADING EXIT *name*

Explanation: RACF attempted to load the RACF exit routine, but could not find this installation-defined module. This error message might indicate a system integrity exposure.

User Response: Report the exact text of this message to your system programmer.

ICH66109I NO PROFILE EXISTS FOR DATA SET *name*

Explanation: Although the RACF indicator for the specified data set is on, no resource profile or UACC has been defined.

User Response: Report the exact text of this message to your system programmer.

ICH66110I NO ENTRIES IN THE RACF CLASS DESCRIPTOR TABLE

Explanation: No entries were found in the class descriptor table supplied by IBM or the installation class descriptor table.

System Action: RACF processing does not occur. Processing continues with the next function.

User Response: Report this message to your RACF security administrator.

ICH66111I RACF GLOBAL ACCESS TABLE NOT FOUND

Explanation: DSMON could not locate the global access table.

System Action: It does not execute function RACGAC, which obtains the entry name and global-access authority level for all classes eligible for global access checking. DSMON continues processing with the next function.

User Response: See your system programmer.

ICH66112I An error occurred during retrieval of LNKST libraries

Explanation: The data security monitor encountered an error while attempting to retrieve a list of LNKST libraries.

System Action: Processing continues with the next function.

User Response: Contact your system programmer.

ICH66134I • ICH66141I

System Programmer Response: This message indicates a probable RACF or MVS error. Contact the IBM support center for assistance.

ICH66134I USER NOT AUTHORIZED TO RECEIVE USERCAT LISTING

Explanation: You do not have the required authority to profile ICHDSM00.SYSCAT in class FACILITY.

System Action: DSMON only reports on the master catalog. No report is made on the user catalogs.

User Response: See your RACF security administrator.

ICH66136I MAXIMUM NUMBER OF PROCESSABLE USRDSNS FOR CURRENT REGION SIZE EXCEEDED

Explanation: DSMON did not execute successfully, because of storage constraints.

System Action: The job ends with return code 8.

User Response: Notify your system programmer.

Programmer Response: See accompanying ICH66137I message.

ICH66137I EITHER INCREASE THE REGION SIZE AND RERUN THE JOB OR RUN A MULTISTEP JOB

Explanation: Not enough storage was available, given the current JCL REGION parameter, for DSMON to process all user data sets as specified.

System Action: The job ends with return code 8.

User Response: Notify your system programmer.

Programmer Response: The job may run successfully if a larger REGION can be specified. If this is impossible, or if the job fails with larger REGIONS, submit a multistep job, breaking up the user data sets into portions as indicated by the messages that follow this one. If possible, isolate the USRDSN USEROPTS into their own steps. If a substantial number of RACGRP USEROPTS are specified in the JCL, isolate these into their own jobsteps as well. Steps in which only USRDSNs or RACGRPS are specified should specify FUNCTION USRDSN or FUNCTION RACGRP to avoid the default (FUNCTION ALL) processing.

ICH66138I DUE TO STORAGE CONSTRAINTS, NO USRDSNS MAY BE SPECIFIED

Explanation: DSMON did not run successfully, because of storage constraints.

System Action: The job ends with return code 8.

User Response: Notify your system programmer.

Programmer Response: See accompanying ICH66139I message.

ICH66139I INCREASE THE JOBS REGION SIZE AS MUCH AS POSSIBLE AND RERUN THE JOB

Explanation: So many user options were specified, for the current REGION size, that DSMON cannot process any of the given data sets or groups.

System Action: The job ends with return code 8.

User Response: Notify your system programmer.

Programmer Response: Increase the REGION JCL parameter as much as possible and rerun the job. If this fails, try submitting a multistep job with the user options (data sets/groups) distributed among two or more job steps. Watch for ICH66138I or ICH66137I messages and instructions that might accompany the initial multistep jobs submitted.

ICH66140I PROGRAM PROPERTIES TABLE SCAN (IEFPPSCN) ERROR

Explanation: An error was returned to the data security monitor (DSMON) from the program properties table scan service (the IEFPPSCN macro).

System Action: The job ends with return code 16.

User Response: Notify your system programmer.

System Programmer Response: This failure may be due to a dynamic Program Properties Table update. Rerun DSMON to see if the problem persists.

ICH66141I UNEXPECTED ICHEINTY ERROR, RC = *retcode*, RSN = *rsncode*, ENTRY = *entry_name* [(G)].

Explanation: This message is issued when processing the RACSPT (started procedure table) report during execution of DSMON (ICHDSM00). An unexpected error occurred from an ICHEINTY macro used to retrieve information for the STDATA segment for a profile in the STARTED class. This message gives the decimal return and reason codes, and the profile name from the RACF database that caused the error, or that was last processed. If the profile name is generic, it is followed by (G).

System Action: The RACSPT report consists of two phases when the STARTED class is active. Phase 1 processes the STARTED class and phase 2 processes the started procedures table (ICHRIN03). Phase 1 has ended and processing continues normally with phase 2. Message ICH66102I (with error code 1) is issued to SYSPRINT to record the unsuccessful completion of part of the RACSPT report. At the conclusion of processing, ICHDSM00 ends with a return code of 16.

User Response: Show the SYSPRINT and SYSUT2

output of ICHDSM00 to your system programmer.

System Programmer Response: Use the return and reason code information in *z/OS Security Server RACF Macros and Interfaces* and the profile name to determine the error condition and fix the error. If necessary, contact the IBM support center.

RACF miscellaneous messages

ICH70001I *userid* **LAST ACCESS AT** *hh:mm:ss* **ON**
day_of_week, month, day, year

Explanation: This message displays the last date and time that user *userid* accessed the system. Some examples are:

- The last date and time user *userid* logged on successfully
- The last date and time a batch job submitted by user *userid* began executing
- The last date and time user *userid* submitted a batch job with JES(EARLYVERIFY) specified on the SETROPTS command

When a user logs on for the first time or for the first time after the RESUME date, the date and time are displayed in asterisks. For example, hh:mm:ss is displayed as **:**:**.

Notes:

1. This message does not reflect all accesses done through APPC.
2. This message is suppressed for started procedures because of a time lapse between the time the procedure starts and when its JOBLOG is activated. It is replaced by MVS message IEF693I or IEF695 identifying the started procedure and its associated user and group ID.

Information in the message includes hour, minute, second, day of week, month, day, and year.

The first time this message is issued for a user, the message is written **:**:** ON ***,** **,****.

This message is routed to the RACF-defined user indicated by *userid* and is issued only when the INITSTATS option (specified on the SETROPTS command) is active.

ICH70002I **YOUR PASSWORD WILL EXPIRE IN** *xxx*
DAYS

Explanation: Your password will expire within the specified number of days. RACF issues this message when the WARNING option on the PASSWORD keyword (specified on the SETROPTS command) is active.

One purpose of this message is to alert a batch user that the password on the JCL statements must be changed within *xxx* days.

ICH70003I **YOU HAVE EXCEEDED THE MAXIMUM
NUMBER OF RACF PASSWORD
ATTEMPTS**

Explanation: You have exceeded the number of consecutive unsuccessful password attempts your installation allows.

System Action: RACF revokes the user ID.

User Response: To reactivate the user ID, see your RACF security administrator.

ICH70004I **USER**(*accessor*) **GROUP**(*group-name*)
NAME(*user-name*) **ATTEMPTED**
'*access-type*' **ACCESS OF ENTITY**
'*resource-name*' **IN CLASS** '*class-name*'
AT *hh:mm:ss* **ON** *month day, year*

Explanation: This message alerts a RACF user that an access violation has occurred against the indicated resource. This message is routed to the user specified in the NOTIFY field of the resource profile that denied the access.

Note: The lines of message text can appear in any order.

The message itself supplies the following information:

accessor

A user ID, job name, or started task name

group-name

A group of which the user is a member

access-type

The intended type of access, such as ALTER, CONTROL, UPDATE, EXECUTE, or READ

resource-name

A resource name, such as a data set name or a volume serial number

Note: The entity name is blank if the authorization check is done for a class in which there are no profiles, such as DIRAUTH.

class-name

One of the valid RACF class names.

The message also indicates the time and date of the violation.

ICH70005I Session attempt rejected. Reason code = *xx*, entity *netid.luid1.luid2*, profile *profile-name*, at *hh:mm:ss* on month, day, year

Explanation: An attempt by logical unit (LU) *netid.luid1* to establish a session with the logical unit *luid2* has been rejected for a security reason. The entity *netid.luid1.luid2* was covered by profile *profile-name*. The message is routed to the user specified in the NOTIFY field of the profile.

System Action: The session stops.

Operator Response: Notify the RACF security administrator of the exact text of the message.

Problem Determination: Check the reason code in the message for one of the following values:

- 02** Local LU (*luid1*) session key will expire in 5 days or less.
- 03** Partner LU's (*luid2*) access has been revoked.
- 04** Session key does not match partner LU (*luid2*) session key.
- 05** Partner LU (*luid2*) stops the session due to a security reason.
- 06** Partner LU (*luid2*) verification required but no session key is defined on this system.
- 07** Possible security attack by partner LU (*luid2*).
- 08** Verification was not indicated by partner LU (*luid2*), but a session key exists on this system.
- 09** Verification was indicated by partner LU (*luid2*), but a session key does not exist on this system.
- 10** Failure due to SNA-security-related protocol error.
- 11** Failure due to profile change during verification.
- 12** The profile has an expired session key.

ICH70006I Userid *userid* associated with procedure [*procname*]*UNKNOWN] has been revoked from [the system|group *groupname*]; verification for the procedure continues.

Explanation: During verification of a started procedure, user ID *userid* associated with procedure *procname* was determined to be revoked from either the system or group *groupname*.

A value of *UNKNOWN for *procname* indicates that the procedure name could not be determined.

If *procname* is blank, the procedure name is made up of at least one non-printable character, which could indicate an error in the procedure name specification.

System Action: The revoked status of the user ID is ignored, and verification processing for the procedure continues.

User Response: Notify your system programmer.

System Programmer Response:

- If the user ID is not intended to be revoked, use the RESUME operand of the ALTUSER command to reinstate the user ID. After the user ID is reinstated, this message will no longer appear.
- If the user ID is intended to be revoked, update the started procedures table (ICHRIN03) to associate another user ID with the procedure. The update will not take place until the next IPL, so this message might appear if the procedure is started again before the next IPL.

ICH70007I USER AUTHORITY CANNOT BE USED FOR THIRD-PARTY AUTHORIZATION CHECK FOR USER (*userid*) GROUP (*groupid*) BECAUSE THE EXECUTION NODE (*nodeid*) IS NOT LOCAL. UACC WILL BE USED.

Explanation: A third-party RACROUTE REQUEST=AUTH call was made specifying an execution node (*nodeid*). However, this execution node was not identified as a local node in the &RACLNDE profile in the RACFVARS class. The user's identity (*userid*) cannot be assumed to be valid at the current node, so the UACC authority for the protected resource is used. If that authority is not sufficient to allow access to the resource, message ICH408I is issued along with this message.

System Action: RACF uses the UACC authority for the protected resource.

System Administrator Response: Check to see if the execution node is supposed to be local. If it is, make sure the node is defined to the &RACLNDE profile in the RACFVARS class. Otherwise only the UACC authority for the protected resource can be obtained.

Miscellaneous RACF ICH Messages

Chapter 4. IRR RACF database initialization messages

This section lists the RACF messages issued by the IRRMIN00 utility during the initialization of the RACF database. The messages are routed to SYSOUT.

The format of the messages is:

IRR8nnn text

where:

IRR identifies the message as a RACF message.
8 identifies the RACF database initialization utility program (IRRMIN00).
nnn is the message serial number.
text is the text of the message.

IRR8000 Maximum number of template definitions exceeded.

Explanation: During initialization of the RACF database, more than 10 template definitions were found on the control card input from the data set defined by the SYSTEMP DD statement.

System Action: Initialization of the RACF database stops.

Operator Response: Report this message to your system programmer.

Programmer Response: Ensure that no more than 10 template definitions exist in the data set defined by the SYSTEMP DD statement. Rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the cause of the problem.

IRR8001 Template is a duplicate. It is ignored.

Explanation: During initialization of the RACF database, two template definitions were found in the data set defined by the SYSTEMP DD statement with the same template number.

System Action: Initialization of the RACF database continues using the first definition of the duplicate pair.

Operator Response: Report this message to your system programmer.

Programmer Response: If the second definition of the duplicate pair is the correct definition, delete the first definition and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the cause of the problem. The template number of the duplicate template is contained in the data statement listed before this message.

IRR8002 RACF data base initialization complete.

Explanation: The RACF database has been successfully initialized.

System Action: Processing continues.

IRR8003 Non-numeric character in numeric field of last statement.

Explanation: During the initialization of the RACF database, an invalid character was found in a numeric field of the previous input statement.

System Action: Initialization of the RACF database stops.

Operator Response: Report this message to your system programmer.

Programmer Response: Ensure there are valid characters in the numeric fields and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the cause of the problem.

IRR8004 RACF data base initialization terminated in error.

Explanation: Initialization of the RACF database has failed (as noted by a previous message).

System Action: Initialization of the RACF database stops.

IRR8005 Beginning RACF data base initialization.

Explanation: Initialization of the RACF database has begun and template definitions will follow.

System Action: Processing continues.

IRR8006 Unable to open DD *ddname*

Explanation: The data set associated with the indicated *ddname* could not be opened.

System Action: Initialization of the RACF database stops.

Operator Response: Report this message to your system programmer.

Programmer Response: Ensure that the DD statement for the indicated data set is correct.

IRR8007 End of file reached before *\$/END* statement.

Explanation: During the initialization of the RACF database, an end-of-file condition was detected on the data set defined by the SYSTEMP DD statement before a *\$/END* statement.

System Action: Initialization of the RACF database continues.

Operator Response: Report this message to your system programmer.

Programmer Response: Verify the contents of IRRTEMP1. If more template definitions were expected, the program must be rerun with the complete set of template definitions as input. If all template definitions are present and only the *\$/END* statement is missing, the program need not be rerun.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the required templates.

IRR8008 End of file reached before end of template definition.

Explanation: In attempting to initialize the RACF database, the end-of-file was encountered before a *\$/TEMPLATE* statement was found.

System Action: The RACF database is not initialized.

Operator Response: Report this message to your system programmer.

Programmer Response: Correct IRRTEMP1 and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the required templates.

IRR8009 Invalid JCL parameter: *parameter*

Explanation: The indicated parameter value is not a valid value for the NEW or UPDATE parameter. Only the first nine characters of the parameter value are listed.

System Action: Updating of the RACF database stops.

Operator Response: Report this message to your system programmer.

Programmer Response: Correct the value specified on the NEW or UPDATE parameter and rerun the program.

IRR8010 Unable to retrieve data base name.

Explanation: While attempting to retrieve the database name allocated by way of the SYSRACF DD statement, an error was encountered from the SVC 99 information retrieval function.

System Action: Updating of the RACF database stops.

Operator Response: Notify the system programmer.

Programmer Response: Correct the SYSRACF DD statement and rerun the program.

IRR8011 RACF data base header record is invalid.

Explanation: The RACF database initialization program found an invalid ICB (header) record in the RACF database while preparing to update the RACF database.

System Action: Updating of the RACF database stops.

Operator Response: Report this message to your system programmer.

Programmer Response: If the RACF database was not previously formatted by way of this program with the PARM='NEW' specification on MVS or with the RACINITD EXEC on z/VM, then rerun the program with PARM='NEW'. If the RACF database is a version 1, release 1 or 2 database that is being updated, then run the RACF database verification utility program (IRRUT200) to determine which ICB field is in error.

Problem Determination: The validity check which caused the failure can result from an invalid ICB value for the number of templates or BAMs, or an invalid RBA (relative byte address). List the contents of the data set defined by the SYSRACF DD statement to determine the cause of the problem.

IRR8012 RACF data base updates complete.

Explanation: The template update function of the RACF database initialization program has completed successfully.

System Action: Processing continues.

IRR8013 RACF data base updates terminated in error.

Explanation: The template update function of the RACF database initialization program ended unsuccessfully as stated in a previous message.

System Action: Updating of the RACF database stops.

Operator Response: Report this message to your system programmer.

Programmer Response: Respond to the previous message and rerun the program.

IRR8014 Segment definition missing from preceding data.

Explanation: In attempting to initialize the RACF database, a \$/TEMPLATE statement was found immediately following a \$/SEGMENT statement.

System Action: The RACF database is not initialized.

Operator Response: Notify the system programmer.

Programmer Response: Correct IRRTEMP1 and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to verify the definitions.

IRR8015 Consecutive segment identifiers.

Explanation: In attempting to initialize the RACF database, a \$/SEGMENT statement was immediately followed by a \$/SEGMENT statement.

System Action: The RACF database is not initialized.

Operator Response: Report this message to your system programmer.

Programmer Response: Correct IRRTEMP1 and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to verify the definitions.

IRR8016 Segment identifier missing from preceding data.

Explanation: In attempting to initialize the RACF database, a field definition statement was found immediately following a \$/TEMPLATE statement.

System Action: The RACF database is not initialized.

Operator Response: Report this message to your system programmer.

Programmer Response: Correct IRRTEMP1 and rerun the program.

Problem Determination: List the contents of the data

set defined by the SYSTEMP DD statement to verify the definitions.

IRR8017 Consecutive template identifiers.

Explanation: In attempting to initialize the RACF database, a \$/TEMPLATE statement was found immediately following a \$/TEMPLATE statement.

System Action: The RACF database is not initialized.

Operator Response: Report this message to your system programmer.

Programmer Response: Correct IRRTEMP1 and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to verify the definitions.

IRR8018 \$/END follows a segment identifier.

Explanation: In attempting to initialize the RACF database, a \$/END statement was found immediately following a \$/SEGMENT statement.

System Action: The RACF database is not initialized.

Operator Response: Report this message to your system programmer.

Programmer Response: Correct IRRTEMP1 and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to verify the definitions.

IRR8019 \$/END follows a template identifier.

Explanation: In attempting to initialize the RACF database, a \$/END statement was found immediately following a \$/TEMPLATE statement.

System Action: The RACF database is not initialized.

Operator Response: Report this message to your system programmer.

Programmer Response: Correct IRRTEMP1 and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to verify the definitions.

IRR8020 Dataset specified for UPDATE function is incorrect.

Explanation: The data set defined by the SYSRACF DD statement for the IRRMIN00 utility does not have a blocksize of 4096.

System Action: Updating of the RACF database is ended.

IRR8021 • IRR8022

Operator Response: Notify the system programmer.

System Programmer Response: Make sure that the data set specified by the SYSRACF DD statement is a valid RACF data set. Rerun the IRRMIN00 utility.

IRR8021 The UPDATE parameter is not permitted while the system is in read-only mode.

Explanation: UPDATE attempts to update the data set templates. However, the database cannot be updated while the system is in read-only mode.

System Action: The RACF database is not initialized. Utility processing stops.

System Programmer Response: You can do one of the following:

- Run IRRMIN00 with a parameter of UPDATE from another system that is not in read-only mode.
- Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
- Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode, then rerun the job.

IRR8022 A coupling facility related error occurred during database UPDATE processing. Utility processing has ended abnormally.

Explanation: An error occurred when accessing the coupling facility. IRRMIN00 PARM=UPDATE has been run against an active data set while the system was in data sharing mode. The IRRMIN00 updates to DASD have been completed, but the ICB has not been updated in the coupling facility.

System Action: IRRMIN00 processing ends abnormally.

System Programmer Response: Check the SYSPRINT. Also, check the information specified in message IRRX016I, which is issued to the system console.

You can do one of the following:

- Rerun the job from the original system if it is still in data sharing mode.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode.
- Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode, then rerun the job.

Chapter 5. IRR messages for the system operator

This section lists the messages with a prefix of IRR that go to the system operator. The format of these messages is:

`IRR x nn t text`

where:

IRR identifies the message as a RACF message.
 x identifies the function issuing the message.
 nn is the message serial number.
 t is the type code (I = information, or A = action).
 $text$ is the text of the message.

Routing and descriptor codes

The routing and descriptor codes for these messages are shown with the message explanations. When there is no destination indicated, the message is returned to the user. Only the messages that go to the operator console have a destination section.

Descriptor code descriptions

Descriptor codes indicate the significance of a message. Specifically, descriptor codes let the user know the status of the system itself or that of a specific task:

Has it stopped processing?
Is it waiting for another action to be completed?
Or, is it continuing to process?

In addition, this code determines how the system will display and delete the message.

Code	Description
------	-------------

1	System Failure
----------	-----------------------

The message indicates a catastrophic error. To continue, the operator must re-IPL the system or restart a major subsystem.

2	Immediate Action Required
----------	----------------------------------

The message indicates that the operator must perform an action immediately. The message issuer could be in a wait state until the action is performed, or the system needs the action as soon as possible to improve performance. The task waits for the operator to complete the action.

Note: When an authorized program issues a message with descriptor code 2, a DOM macro instruction *must* be issued to delete the message after the requested action is performed.

4	System Status
----------	----------------------

The message indicates the status of a system task or of a hardware unit.

5	Immediate Command Response
----------	-----------------------------------

The message is issued as an immediate response to a system command. The response does not depend on another system action or task.

6	Job Status
----------	-------------------

The message indicates the status of a job or job step.

11	Critical Eventual Action Required
-----------	--

IRR008I • IRR009I

The message indicates that the operator must perform an action eventually, and the action is important enough for the message to remain on the display screen until the action is completed. The task does not wait for the operator to complete the action.

Note: Some RACF messages list a destination containing a descriptor code, but indicate that no routing codes are specified for the message. These messages are issued with a command and response token (CART) and console id (CONSID) to direct them to a specific console.

Routing code descriptions

Routing codes send system messages to the consoles where they are to be displayed. To send a message to more than one console, RACF assigns more than one routing code to the message. For more information on message routing, see your MVS routing and descriptor codes manual.

Code Description

1 Master Console Action

The message indicates a change in the status of the system. It requires action by the master console operator.

2 Master Console Information

The message indicates a change in the status of the system. It does not require action; rather, it alerts the master console operator to a condition that may require action.

This routing code is used for any message that indicates job status when the status is not requested specifically by an operator inquiry. It is also used for processor and problem program messages to the system operator.

9 System Security

The message gives information about security checking, for example, a request for a password.

11 Programmer Information

The message is intended for the problem programmer. This routing code is used only when the program issuing the message cannot route the message to the programmer by way of the system output (SYSOUT) data set. The message appears in the job log.

Note: Routing code 11 is ignored if specified for a multiple-line WTO macro instruction.

VERIFY and VERIFYX messages

IRR008I JOB FAILED. USER PARAMETER REQUIRED ON JOB STATEMENT.

Explanation: A job was submitted with no user ID information specified or propagated from the submitter and the system requires jobs to run with RACF user IDs by way of the SETROPTS JES(BATCHALLRACF) or JES(XBMALLRACF) options.

System Action: The job stops. No steps are executed.

User Response: Do one of the following:

- Specify USER parameter on the JOB card
- Change JES(XBMALLRACF) to JES(NOXBALLRACF)
- Change JES(BATCHALLRACF) to JES(NOBTACHALLRACF)

Resubmit the job.

IRR009I JOB FAILED. OLD PASSWORD REQUIRED WITH NEW PASSWORD ON PASSWORD PARAMETER.

Explanation: The old password is missing on the PASSWORD parameter on the JOB statement.

System Action: The job ends with no steps executed.

User Response: Specify both the old password and the new password on the JOB card, PASSWORD=(old,new); and resubmit the job.

IRR010I USERID *userid* IS ASSIGNED TO THIS JOB.

Explanation: The user did not specify the USER parameter on the job card.

System Action: The submitting user's user ID is assigned to this job. (This is normal for user ID propagation.) Processing continues. This message goes only to the job log.

User Response: None.

IRR011I SECLABEL *seclabel* IS ASSIGNED TO THIS JOB.

Explanation: The user did not specify the SECLABEL parameter on the JOB card.

System Action: The security label assigned to the job is the one the submitter is currently using. Processing continues.

User Response: None.

IRR012I VERIFICATION FAILED. USER PROFILE NOT FOUND.

Explanation: There is no user profile in the RACF database for the user associated with this job.

System Action: The external security manager has failed the request. The application decides whether to end the job or continue with an alternative method.

User Response: If the application allows the job to continue, no action is required. Otherwise, specify a RACF-defined user on the USER parameter, or submit from a RACF-defined session.

IRR013I VERIFICATION FAILED. INVALID PASSWORD GIVEN.

Explanation: The password supplied was not contained in the user's profile.

System Action: The job ends with no steps executed.

User Response: Specify the correct password in the PASSWORD parameter on the JOB card.

IRR014I VERIFICATION FAILED. EXPIRED PASSWORD GIVEN.

Explanation: The user's password has expired. A new password must be provided.

System Action: The job ends with no steps executed.

User Response: Specify a new password with the old expired one on the JOB card: PASSWORD=(old,new).

IRR015I VERIFICATION FAILED. NEW PASSWORD IS NOT VALID.

Explanation: The new password is not valid or is the same as the old password.

System Action: The job ends with no steps executed.

User Response: Specify a valid new password. For assistance with your installation's password rules, see your RACF security administrator.

IRR016I VERIFICATION FAILED BY RACF INSTALLATION EXIT.

Explanation: The job was failed by the RACINIT installation exit routine taken when the job was initiated.

System Action: The job ends with no steps executed.

User Response: Report this message to your RACF system programmer.

IRR017I VERIFICATION FAILED. USER IS REVOKED AT THE GROUP LEVEL.

Explanation: The group specified (which is either the default group or is specified on the job card) is a valid group for this user. However, the user's access to the group has been revoked.

System Action: The job ends with no steps executed.

User Response: Report this message to your RACF security administrator.

IRR018I VERIFICATION FAILED. OIDCARD IS REQUIRED.

Explanation: The user is required to supply an operator ID card when entering the system. It is not possible to supply an OIDCARD with this batch job.

System Action: The job ends with no steps executed.

User Response: Specify a different user on the JOB card.

RACF processing messages

IRR401I *abend-code* **ABEND DURING RACF PROCESSING OF** *request-name*
REQUEST FOR ENTRY *entry-name* **[IN**
CLASS *class-name* **][{PRIMARY |**
BACKUP } RACF DATA SET
SEQUENCE *nnn, dsname* **--or-- I/O**
ERROR AT RBA *relative-byte-address*
DURING RACF PROCESSING OF
request-name **REQUEST FOR ENTRY**
entry-name **[IN CLASS** *class-name* **]**
[{PRIMARY | BACKUP } RACF DATA
SET SEQUENCE *nnn, dsname* **--or--**
RESTART KEY HIT DURING RACF
PROCESSING OF *request-name*
REQUEST FOR ENTRY *entry-name* **[IN**
CLASS *class-name* **][{PRIMARY |**
BACKUP } RACF DATA SET
SEQUENCE *nnn, dsname*]

Explanation: An abend or an I/O error occurred during RACF processing, or the restart key was pressed.

relative-byte-address

The RBA (relative byte address) where the I/O error occurred.

request-name

The type of request the RACF manager was processing when the error occurred.

class-name

For resources other than DASD data sets, the class name of the resource. The 8-character class name and a hyphen precede the entry name zzz in the RACF database index. For example, the index name of TAPEVOL -T12345 is used to locate profile T12345 in class TAPEVOL.

dsname and nnn

If more than one RACF database exists, *dsname* and *nnn* indicate the database and sequence number affected.

System Action: The indicated request to the RACF manager failed. RACF stops processing the request.

Operator Response: Save the exact text of this message and of any following RACF messages (particularly IRR413I), and report them to the system programmer or the RACF security administrator, or both.

Programmer Response: If message IRR402I, IRR403I, or IRR404I does not follow this message at the security console, the error occurring in the RACF database may not represent a permanent error. Attempt to reenter the RACF request (either the RACF command or the utility program), or cause the RACF SVC to be invoked again (such as reentering the LOGON command, rerunning the job, or retrying dynamic allocation).

If message IRR402I, IRR403I, or IRR404I does follow this message, then a permanent error may exist in the RACF database. Perform the action as specified by the problem determination section for that message.

If an I/O error is occurring frequently on the RACF database, an alternate device could be considered for the next IPL.

If multiple extents were created for a new RACF database, this message is issued when the new database is used. Delete the database and rerun the IRRMIN00 utility to recreate it. Specify CONTIG and do not specify secondary space on the SPACE parameter in the JCL.

Problem Determination: If an abend occurred, do the following:

- Get the abend code from this message. If the abend is 000, see other messages issued for this problem (such as ICH409I) for the abend code.
- Look for a description of the abend code in the following places:
 - Chapter 8, “RACF abend codes” on page 295
 - *z/OS MVS System Codes*.

If you cannot find the abend code described in any of the above, use the *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing documentation errors and reporting documentation errors to IBM.

Diagnostic data is provided in the LOGREC data.

If an I/O error occurred, determine if the device or volume is malfunctioning. For a permanent I/O error, also see the LOGREC data for diagnostic information. Also, see the section on failure during I/O operations on the RACF database in *z/OS Security Server RACF System Programmer's Guide*.

If message IRR402I, IRR403I, or IRR404I follows this message, see “Problem Determination” for that message.

Destination: Descriptor code is 6 for x3E and x22 abends and 1 for all other abends. Routing codes are 9 and 11. The complete text of this message is sent only to the security console. Only IRR401I *abend-code* ABEND DURING RACF PROCESSING is sent to the programmer.

IRR402I **BAM BLOCK AT RBA**
relative-byte-address **MAY NOT**
REFLECT ACTUAL SPACE USAGE

Explanation: An error has occurred during RACF processing when attempting to allocate or deallocate space in the RACF database. The BAM block at the

RBA (relative byte address) indicated in the message may not be accurate.

This message follows message IRR401I. If more than one RACF database exists, the database referred to in this message is the database named in the preceding IRR401I message.

System Action: RACF processing of the request indicated in message IRR401I ends.

Operator Response: Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

Programmer Response: See “Problem Determination.”

Problem Determination: The control information in the RACF database may not be accurate. Execute the RACF database verification utility program IRRUT200 to determine the inconsistency between the BAM mappings and the actual space allocated.

If an inconsistency is found, use the BLKUPD command to correct the BAM blocks so they accurately reflect the space allocated. See the *z/OS Security Server RACF Diagnosis Guide* for additional information on how to diagnose and correct problems with BAM blocks.

Destination: Descriptor code is 4. Routing code is 9.

**IRR403I INDEX MAY BE INVALID; LEVEL *nn*
INDEX BEING PROCESSED FOR
{ADDITION | DELETION} AT TIME OF
FAILURE**

Explanation: An error occurred during RACF updating of the index in the RACF database. The level index being processed is indicated by *nn*. This message follows message IRR401I. If more than one RACF database exists, the database referred to in this message is the database named in the preceding IRR401I message.

System Action: RACF stops processing the request indicated in message IRR401I.

Operator Response: Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

Programmer Response: See “Problem Determination.”

Problem Determination: The control information in the RACF database may not be accurate. Execute the RACF database verification utility program IRRUT200. To determine if there is an inconsistency in the index structure.

If an inconsistency is found, use the BLKUPD command to correct the index structure so that it accurately reflects the contents of the RACF database. See *z/OS Security Server RACF System Programmer's Guide* for additional information on how to diagnose and correct

problems with the data set index.

Destination: Descriptor code is 4. Routing code is 9.

**IRR404I ICB RECORD HAS NOT BEEN
UPDATED - {TOP LEVEL INDEX |
SEQUENCE SET } RBA IS INCORRECT**

Explanation: An error occurred during RACF processing. The header record (ICB) in the RACF database had not been updated before the failure occurred in the RACF database. Updates to the index structure (that is the top level index block or the beginning of the sequence set) are not reflected in the ICB. The latest updates to the index will not be reflected in searches of the RACF database.

This message follows message IRR401I. If more than one RACF database exists, the database referred to in this message is the database indicated in the preceding IRR401I message.

System Action: RACF stops processing the request.

Operator Response: Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

Programmer Response: See “Problem Determination.”

Problem Determination: The control information in the RACF database may not be accurate. Execute the RACF database verification utility program IRRUT200 to determine if there is an inconsistency in the ICB and index structure. If an inconsistency is found, use the BLKUPD command to update the ICB so that it accurately reflects the contents of the index structure. See the *z/OS Security Server RACF Diagnosis Guide* for additional information on how to diagnose and correct problems with the data set index.

Destination: Descriptor code is 4. Routing code is 9.

**IRR405I INSUFFICIENT SPACE ON RACF DATA
SET [{PRIMARY | BACKUP } RACF
DATA SET SEQUENCE *nnn*, *dsname*]**

Explanation: The RACF data set does not contain sufficient contiguous space to handle the RACF request. Either there is insufficient space available in the RACF data set or the available space has become too fragmented to satisfy the request.

If the RACF database is comprised of more than one data set, *dsname* with sequence number *nnn* is the data set that encountered the error.

System Action: RACF stops processing the request.

Operator Response: Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

Programmer Response: See “Problem Determination.”

IRR406I • IRR407I

Problem Determination: Execute the RACF database verification utility program IRRUT200 to determine:

- The amount of available space in the RACF data set
- Whether significant fragmentation has occurred

If more space is needed, delete any unused profiles from the RACF data set. This might allow the request to succeed when you try again. If that is not sufficient, use the RACF database utility program IRRUT400 to rebuild the RACF data set and enlarge it if necessary. See *z/OS Security Server RACF System Programmer's Guide* for information on the IRRUT200 and IRRUT400 utilities and for information on monitoring the RACF database to help you prevent future insufficient space conditions.

Destination: Descriptor code is 4. Routing codes are 2, 9, and 11.

IRR406I RACF DATA SET INDEX FULL
[(PRIMARY | BACKUP) RACF DATA
SET SEQUENCE *nnn, dsname*]

Explanation: During RACF processing, an attempt was made to extend the index to another level, but the maximum number of index levels (10) had been reached.

If the RACF database is comprised of more than one data set, this message indicates which data set the error occurred on.

System Action: RACF stops processing the request.

Operator Response: Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

Programmer Response: See "Problem Determination."

Problem Determination: Execute the RACF database verification utility program IRRUT200 to determine the index structure and index levels. Delete unused profiles to reduce the number of index entries and make space available. If an error in the index structure is suspected, execute the RACF database verification utility program IRRUT200 to determine if there is an inconsistency.

If an inconsistency is found, use the BLKUPD command to correct any problems in the index of the RACF database. RACF allows a maximum of 10 index levels. See *z/OS Security Server RACF Diagnosis Guide* for additional information on how to diagnose and correct problems with the data set index.

Destination: Descriptor code is 4. Routing codes are 9 and 11.

IRR407I RACF DATA SET INDEX ERROR.
[(PRIMARY | BACKUP) RACF DATA
SET SEQUENCE *nnn, dsname*] SEARCH
ON ENTRY *entry-name*

Explanation: An index error in the RACF database was detected while RACF was performing an index search for the entry indicated in the message. This message is issued if:

- During the index search, a block is found which is not an index block.
- The data pointed to by a level one index block is not the entry for the entry name indicated in the message.

If more than one RACF database exists, this message indicates which database the error occurred on.

System Action: RACF stops processing the request.

Operator Response: Report the exact text of this message to your system programmer or the RACF security administrator, or both.

System Programmer Response: See "Problem Determination."

Problem Determination: Execute the RACF database verification utility program IRRUT200 to determine the error in the index tree in the RACF database.

If the IRRUT200 utility does not find the error, list the profile indicated in the message by *entry-name*, using the appropriate RACF command. For example, if the search was for user profiles, use the LISTUSER command. If CLASS was not specified on the SEARCH command, use the LISTDSD command. Look for error messages such as NO CONNECT ENTRY FOUND or invalid data in fields such as OWNER.

To correct any errors found, use the BLKUPD command. See *z/OS Security Server RACF Diagnosis Guide* for additional information on how to diagnose and correct problems with the data set index.

If you found no errors, it is possible that an in-storage overlay problem occurred, during which an index block was overwritten. Try solving the problem by flushing and rebuilding the in-storage buffers, by INACTIVATING and then REACTIVATING the appropriate RACF database(s) using the RVARY command. Be careful not to inadvertently drop the system into RACF FAILSOFT processing. You should also be aware that if you switch the primary database to the backup database, reactivate the old primary database and then switch back. There is a potential for the databases to be out of synchronization. Either do this procedure at a quiesced activity time or consider using the IRRUT200 utility, properly employed, to resynchronize them. See the *z/OS Security Server RACF Command Language Reference* for details on RVARY usage and the *z/OS Security Server RACF System Programmer's Guide* for information on the IRRUT200 utility.

Destination: Descriptor code is 4. Routing codes are 9 and 11.

**IRR410I RACF UNABLE TO BACK UP UPDATE
OF *entry-name* BACKUP RACF DATA
SET SEQUENCE *nnn*, *dsname***

Explanation: A failure occurred in attempting to duplicate on the backup RACF database an update performed in the corresponding primary database. The database is identified by:

nnn Database sequence number (1 to 255)

dsname
Database name.

System Action: RACF has not duplicated the update operation. Processing continues.

Operator Response: Notify system programmer.

Programmer Response: See "Problem Determination."

Problem Determination: If this message is preceded by message IRR401I, IRR405I, IRR406I, or IRR407I, the error was encountered on the backup database. Otherwise, the backup database was not in synchronization with its primary database. If the backup database was not in synchronization with the primary database, see *z/OS Security Server RACF System Programmer's Guide* for information on the IRRUT200 and IRRUT400 utilities.

Destination: Descriptor code is 4. Routing code is 9.

**IRR411I MAXIMUM PROFILE SIZE EXCEEDED.
profile-name NOT ALTERED.**

Explanation: During RACF processing, an attempt was made to expand profile *profile-name*. The profile has reached the maximum output size that RACF can handle (65 535 bytes); the profile cannot be made larger.

Note: Although some profiles can be larger for repeat groups, the maximum output length remains at 65 535 bytes.

System Action: RACF stops processing the request.

Operator Response: Report this message to the system programmer or the RACF security administrator, or both, and save this output.

Programmer Response: profile has reached the maximum size allowed. If possible, decrease the size of the profile; if that is not possible, you must split the profile. For example, you could split a group with too many users into several smaller groups.

Destination: Descriptor code is 4. Routing code is 9.

**IRR413I RACF MANAGER REQUEST ID WAS
*request-id***

Explanation: This message contains additional information to help determine the cause of an IRR401I error message. This message is issued only after an IRR401I message. The *request-id* field contains an ID that can help the IBM support center determine the cause of the problem.

System Action: See message IRR401I.

Operator Response: See message IRR401I.

Programmer Response: message IRR401I.

Destination: Descriptor code is 4. Routing codes are 4 and 13.

**IRR416I RACF DETECTED AN INVALID
NON-EGN DATASET PROFILE NAME.
PROFILE *profile-name* DOES NOT
PROTECT THE INTENDED
RESOURCES.**

Explanation: RACF detected a profile that was added before the enablement of Enhanced Generic Names (EGN) and that cannot be interpreted as intended under EGN rules. This message identifies the non-EGN generic data set profile name. Under EGN rules, the profile may not protect the resources that it was defined to protect. If this message is issued during processing of a SEARCH or LISTDSD GENERIC request, bad profile names (particularly names 43 and 44 characters in length) may also have been displayed and the output should be considered unreliable.

For example, suppose the following six generic data set profiles were defined before turning EGN on:

```
1 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.*'
2 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD*'
3 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*'
4 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD*'
5 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.D.*'
6 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD*'
```

Then EGN was enabled and three more generic data set profiles were defined:

```
7 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.*'
8 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.*'
9 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.*'
```

A subsequent SEARCH request would display the following:

IRR417I

```
SEARCH CLASS(DATASET)
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.
A IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.* (G)
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
B IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD* (G)
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.
C IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.** (G)
D IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.* (G)
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*
        DOES NOT PROTECT THE INTENDED RESOURCES.
E IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD* (G)
IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
        PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD*
        DOES NOT PROTECT THE INTENDED RESOURCES.
F IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.** (G)
G IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.D.* (G)
H IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD* (G)
I IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.** (G)
```

RACF command processing may have caused the IRR416I message to be issued more than once. However, any time it is issued during a command invocation, the command output must be considered unreliable. In the example above, changes in EGN rules may have caused RACF to incorrectly interpret non-EGN profiles (1) and (2) as SEARCH profiles (A) and (B). These profiles no longer cover the intended resources. Even though names (D) and (E) appear correct, with no additional characters at the end, they also do not cover the intended resources and cause IRR416I messages to be issued. EGN profiles (7), (8), and (9) were correctly displayed by SEARCH as (C), (F), and (I). Profiles (G) and (H) follow the same rules under non-EGN and EGN, so they actually protect what they were intended to protect.

System Action: RACF processing of the request continues.

Operator Response: Report this message to the system programmer or the RACF security administrator and save the message output.

Programmer Response: See "Problem Determination."

Problem Determination: This message identifies the bad profile.

An EGN profile, possibly less specific, can be defined to protect the desired resources; however the original bad non-EGN profile must still be deleted to prevent further IRR416I messages.

To delete bad profiles:

1. Use SETROPTS NOEGN to temporarily disable EGN. During this time, there should be no other system activity, in order to prevent the creation of generic profiles that could result in additional

problems. Under normal circumstances, it is not recommended that EGN be turned off after it is turned on.

2. Use SEARCH GENERIC CLIST NOMASK NOLIST to create a CLIST containing generic data set profile names.
3. Edit the CLIST, to find 42- and 43-character names ending in '.*'.
4. Delete the profiles found.
5. Use SETROPTS EGN to re-enable EGN.
6. Define profiles according to EGN rules that protect the resources intended to be protected by the non-EGN profile names.

Destination: Descriptor code is 4. Routing codes are 9 and 11. Routing code 11 is only used when a TSO environment is not in effect.

**IRR417I UNABLE TO COMMUNICATE WITH THE
RACF SUBSYSTEM. IEFSSREQ
RETURN CODE IS *return-code*.**

Explanation: RACF attempted to process a password change request for a user. The password change has been made on this system's RACF database. However, if associations exist with another user on this or a remotely connected system, the passwords will not be synchronized. Report this message to your system programmer.

System Action: The system continues processing.

System Programmer Response: The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

Code	Explanation
4	The subsystem does not support this function.
8	The subsystem exists, but is not active.
12	The subsystem is not defined in the IEFSSNxx parmlib member.
16	The function has not completed. This is a disastrous error.
20	The SSOB or SSIB have invalid lengths or formats.
24	The SSI has not been initialized.

A return code of 4, 16, 20 or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See *z/OS Security Server RACF Migration* for installation considerations and *z/OS Security Server RACF System Programmer's Guide* for configuration considerations for the RACF subsystem.

Destination: Descriptor code is 3. Routing codes are 9 and 11.

**IRR418I RACF PRODUCT DISABLED:
{COMMAND | UTILITY | IRRSSM00 |
IRRSSI00 | IRRDPI00} ENDED.**

Explanation: This system is running z/OS Version 1 Release 2 or higher. The RACF initialization process made a registration check based on the IFAPRDxx member in SYS1.PARMLIB. This message implies that:

- The RACF product was not enabled
- RACF initialization did not continue
- Control was given to a RACF command processor, RACF utility, or that initialization was attempted for the RACF subsystem (IRRSSM00 or IRRSSI00) or for RACF's dynamic parse (IRRDPI00)

Note: This message can be sent as:

- A TSO message
- Batch job output
- A console message

System Action: Because RACF is not enabled, the respective process ends. The return code for RACF utilities failing in this way is X'20' (decimal 32).

Destination: Descriptor code is 11. Routing codes are 1 and 9.

**IRR419I ALIAS INDEX ENTRY IS TOO LARGE
FOR TYPE *profile-type* SEGMENT
segment-name FIELD *field-name* ALIAS
alias-value.**

Explanation: An attempt was made to increase the length of an alias index entry. This occurs when an additional user or group profile is being associated with an alias name. Adding the additional user or group would cause the maximum size of the index entry to be exceeded.

System Action: RACF stops processing the request.

User Response: If you are attempting to assign a UID to a user or a GID to a group, select another UID or GID. There are too many base profiles associated with this alias value and no more can be added.

Destination: Descriptor code is 4. Routing code is 9.

IRRDPI00 command messages

**IRR545I IRRDPI00 FAILED BECAUSE IT IS NOT
A TSO-AUTHORIZED COMMAND**

Explanation: This message is issued when the IRRDPI00 UPDATE command is issued from a started task (for example, during IPL), but the IRRDPI00 command is not defined as an authorized command in the IKJTSOxx parameter library member.

System Action: RACF processing continues normally, except that users cannot work with profile segments (such as TSO or DFP segments). This affects both RACF command users and RACF ISPF panel users.

Operator Response: Report this message to your system programmer.

System Programmer Response: Ensure that the IRRDPI00 command is defined as an authorized command in the IKJTSOxx parameter library member.

If the problem persists, call your IBM support center.

**IRR546I *jobname* FAILED. SAVE JOB LOG AND
CONTACT SYSTEM SUPPORT**

Explanation: This message is issued when the IRRDPI00 UPDATE command is issued from a started task (for example, during IPL), and then a problem occurs. The *jobname* is the name of the job used to run dynamic parse.

System Action: RACF processing continues normally, except that users cannot work with profile segments (such as TSO or DFP segments). This affects both RACF command users and RACF ISPF panel users.

Operator Response: Report this message to your system programmer.

System Programmer Response: Check the job log of the started task for other messages that may be related to this problem. Find out what was wrong, correct the problem, and re-IPL.

RACROUTE REQUEST=AUTH VLF messages

**IRR803I VLF IS NOT ACTIVE. POSSIBLE RACF
PERFORMANCE IMPACT**

Explanation: This message appears when VLF is inactive and RACF is doing group authority checking. RACF uses VLF to store group tree information for improving performance.

System Action: RACF will continue processing without using VLF. The result of group authority checking should be the same whether VLF is active or not.

Operator Response: Use operation procedures for your installation to decide whether to activate VLF. The command S VLF,SUB=MSTR will start the VLF, and VLF will use the COFVLF00 PARMLIB member as the default. The command STOP VLF will deactivate VLF.

Destination: Descriptor code is 4. Routing code is 1.

**IRR804I RACF VLF CLASS IRRGTS NOT
DEFINED IN COFVLFxx PARMLIB.**

Explanation: This message appears when VLF is active but the VLF class IRRGTS is not defined in the COFVLFxx parameter library member. Therefore, GTS (group trees in VLF storage) cannot be activated in RACF. It will affect the RACF performance during group authority checking.

System Action: RACF will continue processing without GTS. The result of group authority checking should be the same no matter whether GTS is active or not.

Operator Response: Use the installation procedures

to decide whether or not to activate GTS. If the decision is to have GTS active, update the COFVLFxx PARMLIB member to specify that the VLF class name is IRRGTS and its major name is GTS. Add the following two lines to the COFVLFxx parameter library member.

```
CLASS NAME(IRRGTS)  /* RACF GTS Feature */
EMAJ(GTS)           /* Major Name       */
```

After updating the COFVLFxx PARMLIB, you must activate GTS. One way to make GTS active is to stop VLF, and start it again with the updated COFVLFxx parameter library member.

Destination: Descriptor code is 4. Routing code is 1.

RACROUTE REQUEST=VERIFY NJE messages (Part 1)

Note on NJE Messages

See message IRR815I for an additional NJE operator message.

**IRR805I IDENTITY IS PROPAGATED FOR THE
UNKNOWN USER FROM TRUSTED
NODE *node-name*.**

Explanation: This informational message is sent to the security console when a job is received from an unknown user on a trusted node. The NODES profile lookup for this submitter resulted in a UACC that allowed propagation of the NJE unknown user, set by SETROPTS JES(NJEUSERID(*userid*)). Propagation of this submitter is not possible. This situation can occur when a job is sent across nodes by an external physical reader such as a card reader. Refer to *z/OS Security Server RACF Security Administrator's Guide* for details on the NODES profile lookup. This message occurs only once per IPL; however, an SMF record is cut for every occurrence.

System Action: The job is allowed to run. If a user ID is specified, a password is required and no propagation takes place. If a user ID is not specified, the job runs according to the setting on the SETROPTS JES(BATCHALLRACF) command. Refer to *z/OS Security Server RACF Security Administrator's Guide* for information on using the BATCHALLRACF operand.

Note: When *userid-2* is "&SUSER", it is possible for an additional IRR806I message to be issued, because a second NODES lookup is done. Refer to *z/OS Security Server RACF Security Administrator's Guide* for information about &SUSER.

System Action: Processing continues with the authority of *userid-2*.

**IRR807I PROFILE *profile-name* IN THE NODES
CLASS WAS USED TO TRANSLATE
SECLABEL *seclabel-1* TO *seclabel-2*.**

Explanation: This informational message is sent to the security console when a security label is translated for NJE (network job entry). The *profile-name* is the actual profile used to do the translation. To determine which ENTITY was built, refer to *z/OS Security Server RACF Security Administrator's Guide* for information about NODES profiles.

System Action: Processing continues with *seclabel-2* as the current security label.

**IRR806I PROFILE *profile-name* IN THE NODES
CLASS WAS USED TO TRANSLATE
USER *userid-1* TO *userid-2*.**

Explanation: This informational message is sent to the security console when a user ID is translated for NJE (network job entry). The *profile-name* is the actual profile used to do the translation. To determine which ENTITY was built, refer to *z/OS Security Server RACF Security Administrator's Guide* for information about NODES profiles.

**IRR808I WARNING: NJE SYSOUT ERROR
FROM NODE *nodeid*. USER (*userid-1*)
GROUP (*groupid*) SECLABEL (*seclabel*)
[*poeclass(poeid)*] RACF VERIFYX
RETURN CODE CHANGED FROM *nn* to
0. UNDEFINED USER *undef-user*
ASSIGNED.**

Explanation: Security information was incorrect during NJE SYSOUT verification from the *nodeid* submit node for user *userid-1* using group *groupid*, security label *seclabel*, and if specified, the *poeid* port of entry in the specific *poeclass* port of entry class (such as the

JESINPUT class). Return code *nn* is the hexadecimal value of the return code that describes the error. VERIFYX return codes for RACF are described in *z/OS Security Server RACROUTE Macro Reference*.

System Action: SYSOUT verification continues with the NJE unknown user as specified by SETROPTS JES(NJEUSERID(*undef-user*)).

System Action: Processing continues with *seclabel-2* as the current security label.

RACF user ID and group ID mapping messages

IRR809I VLF CLASS IRRUMAP NOT IN COFVLFxx PARMLIB OF VLF.

Explanation: VLF is active, but the VLF class IRRUMAP is not defined in the COFVLFxx parmlib member. Therefore, the UMAP function of RACF cannot be activated. The performance of UID-to-user ID mapping is affected because a search of the RACF database must be performed to retrieve this information.

System Action: RACF continues processing without using VLF for the UMAP function. The results of the UID-to-user ID mapping are not affected.

System Programmer Response: Use the installation procedures to decide whether to activate the UMAP function. If the decision is to have UMAP active, update the COFVLFxx parmlib member. For the procedure for this, refer to *z/OS Security Server RACF System Programmer's Guide*.

Destination: Descriptor code is 4. Routing code is 1.

IRR810I VLF CLASS IRRGMAP NOT IN COFVLFxx PARMLIB OF VLF.

Explanation: VLF is active, but the VLF class IRRGMAP is not defined in the COFVLFxx parmlib member. Therefore, the GMAP function of RACF cannot be activated. The performance of GID-to-group name mapping is affected because a search of the RACF database must be performed to retrieve this information.

System Action: RACF continues processing without using VLF for the GMAP function. The results of the GID-to-group name mapping are not affected.

System Programmer Response: Use the installation procedures to decide whether to activate the GMAP function. If the decision is to have GMAP active, update the COFVLFxx parmlib member. For the procedure for this, refer to *z/OS Security Server RACF System Programmer's Guide*.

Destination: Descriptor code is 4. Routing code is 1.

Dynamic started task messages

IRR812I PROFILE *profile-name* [(G)] IN THE STARTED CLASS WAS USED TO START *member-name* [WITH JOBNAME *jobname*].

Explanation: An MVS START command was processed. The STARTED class is active and SETROPTS RACLISTed. The indicated profile in the STARTED class has a STDATA segment that specifies TRACE(YES).

Operator Response: Notify the system programmer or security administrator. Tell them the profile name, member name, and job name (if any) contained in the message text.

System Programmer Response: The security administrator responsible for profiles in the STARTED class has requested that message IRR812I be issued whenever the indicated profile is used when processing a START command. The administrator should be informed that this message has occurred.

Destination: Descriptor code is 6. Routing code is 9.

IRR813I NO PROFILE WAS FOUND IN THE STARTED CLASS FOR *member-name* [WITH JOBNAME *jobname*]. RACF WILL USE ICHRIN03.

Explanation: An MVS START command was processed and the STARTED class is active. One of the following problems occurred:

- The STARTED class is SETROPTS RACLISTed, but no profile was found to assign security information for the procedure or job being started.

- A profile to assign security information for the procedure or job being started has been defined, but the STARTED class has not been SETROPTS RACLISTed, or has not been SETROPTS RACLIST REFRESHed on the system where the START command was issued.

System Action: RACF uses the information in the started procedures table (ICHRIN03) to assign security information for this started procedure or job.

Operator Response: Notify the system programmer or security administrator. Tell them the member name and job name (if any) contained in the message text.

System Programmer Response: Do one of the following:

- The security administrator responsible for profiles in the STARTED class has not defined a profile to be used when starting the indicated procedure or job. Inform the administrator that this message has occurred so a profile can be defined, if one is desired.
- Profiles exist or have been defined in the STARTED class for the indicated procedure or job, but the security administrator has not SETROPTS RACLISTed or SETROPTS RACLIST REFRESHed the STARTED class. The administrator should be informed that this message occurred so the STARTED class can be SETROPTS RACLISTed or SETROPTS RACLIST REFRESHed.

Destination: Descriptor code is 6. Routing code is 9.

IRR814I **PROFILE** *profile-name* [(G)] **IN THE STARTED CLASS DID NOT ASSIGN A USERID FOR** *member-name* **[WITH JOBNAME** *jobname* **]. RACF WILL USE ICHRIN03.**

Explanation: An MVS START command was processed. The STARTED class is active and SETROPTS RACLISTed. The profile that matches the procedure name (and job name, if any) did not assign a user ID to be used for the procedure or job being started.

System Action: RACF uses the information in the started procedures table (ICHRIN03) to assign security

information for this started procedure or job.

Operator Response: Notify the system programmer or security administrator. Tell them the profile name, member name and job name (if any) contained in the message text.

System Programmer Response: The security administrator responsible for profiles in the STARTED class has defined an incomplete profile to be used when starting the indicated procedure or job. The administrator should be informed that this message has occurred so the profile can be corrected.

Destination: Descriptor code is 6. Routing code is 9.

RACROUTE REQUEST=VERIFY NJE messages (Part 2)

Note on NJE Messages

Additional NJE operator messages begin with message IRR805I.

IRR815I **PROFILE** *profile-name* **IN THE NODES CLASS WAS USED TO TRANSLATE GROUP** *group-1* **TO** *group-2*.

Explanation: This informational message is sent to the security console when a group ID is translated for NJE (network job entry). The *profile-name* is the actual profile used to do the translation. To determine which entity was built, refer to *z/OS Security Server RACF*

Security Administrator's Guide for information about NODES profiles.

Note: When *group-2* is &DFLTGRP, the user's default group is used for purposes of verification.

System Action: Processing continues with the authority of *group-2*.

VLF cache messages

IRR816I **VLF CLASS 'IRRSMAPI' NOT DEFINED IN COFVLFxx PARMLIB OF VLF.**

Explanation: VLF is active but the VLF class IRRSMAPI is not defined in the COFVLFxx PARMLIB member. Performance during the creation of user security packets (USP) is impacted.

System Action: RACF continues processing without using VLF for the SMAP function. The results of the **initUSP** callable service to create user security packets are not affected.

System Programmer Response: Use the installation procedures to decide whether to activate the SMAP function. If you decide to activate the function, update the COFVLFxx PARMLIB member. To see a procedure for this, refer to *z/OS Security Server RACF System Programmer's Guide*.

Destination: Descriptor code is 4. Routing code is 1.

RACF/DB2 external security module messages

IRR900A **RACF/DB2 EXTERNAL SECURITY MODULE FAILED TO INITIALIZE FOR DB2 SUBSYSTEM** *subsystem-name* **BECAUSE CLASS** *classname* **COULD NOT BE RACLISTED. RACROUTE RETURN CODE** *return_code*, **RACF RETURN CODE** *return_code*, **REASON CODE** *reason_code*.

Explanation: The RACF/DB2 external security module initialization function for DB2 subsystem *subsystem-name* attempted to RACLIST class

classname using RACROUTE REQUEST=LIST,ENVIR=CREATE,GLOBAL=YES. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem. The RACROUTE request failed with the return and reason codes provided in the message text. The return and reason codes are shown in hexadecimal format.

System Action: See System Action for message IRR912I or IRR913I.

Operator Response: Contact the system programmer.

IRR901A • IRR904I

System Programmer Response: Use the RACROUTE return code and RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

**IRR901A RACF/DB2 EXTERNAL SECURITY
MODULE FAILED TO INITIALIZE FOR
DB2 SUBSYSTEM *subsystem-name*
BECAUSE NO ACTIVE DB2 RELATED
CLASSES WERE FOUND.**

Explanation: The RACF/DB2 external security module initialization function for subsystem *subsystem-name* determined that no classes for the indicated DB2 subsystem are active. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

System Action: See System Action for message IRR912I or IRR913I.

Operator Response: Contact your security administrator.

Security Administrator Response: Activate the desired classes for the indicated DB2 subsystem and restart DB2.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

**IRR902A RACF/DB2 EXTERNAL SECURITY
MODULE FAILED TO INITIALIZE FOR
DB2 SUBSYSTEM *subsystem-name*
BECAUSE THE INPUT ACEE WAS
{MISSING | NOT VALID}.**

Explanation: The RACF/DB2 external security module initialization function for subsystem *subsystem-name* determined that the input DB2 subsystem ACEE was either not valid or missing. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

System Action: See System Action for message IRR912I or IRR913I.

Operator Response: Contact the DB2 system programmer.

System Programmer Response: Contact the IBM support center.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

**IRR903A RACF/DB2 EXTERNAL SECURITY
MODULE FAILED TO INITIALIZE FOR
DB2 SUBSYSTEM *subsystem-name*
BECAUSE RACF WAS NOT ACTIVE.**

Explanation: The RACF/DB2 external security module initialization function for subsystem *subsystem-name* determined that RACF is not active on this system. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

System Action: See System Action for message IRR912I or IRR913I.

Operator Response: Contact the RACF system programmer.

Problem Determination: Issue the RVARY LIST command to determine RACF status.

System Programmer Response: Determine why RACF is inactive. After you correct the problem, activate RACF and restart DB2.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

**IRR904I RACF/DB2 EXTERNAL SECURITY
MODULE INITIALIZED WITH
WARNINGS FOR DB2 SUBSYSTEM
subsystem-name BECAUSE A DEFAULT
ACEE COULD NOT BE CREATED.
RACROUTE RETURN CODE
return_code, RACF RETURN CODE
return_code, REASON CODE
reason_code.**

Explanation: The RACF/DB2 external security module initialization function for subsystem *subsystem-name* attempted to create a default ACEE to use in subsequent authority checking when no ACEE is provided. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

The attempt to create the ACEE using RACROUTE REQUEST=VERIFY,ENVIR=CREATE failed with the return and reason codes provided in the message text. The return and reason codes are shown in hexadecimal format.

System Action: Processing continues and the RACF/DB2 external security module is used for subsequent authority checking if DB2 provides an ACEE. If no ACEE is provided, requests are deferred to DB2.

Operator Response: Contact the DB2 system programmer.

System Programmer Response: Use the RACROUTE return code and RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR905I **RACF/DB2 TERMINATION FUNCTION COMPLETED WITH WARNINGS FOR DB2 SUBSYSTEM** *subsystem-name* **BECAUSE CLASS** *classname* **COULD NOT BE UN-RACLISTED. RACROUTE RETURN CODE** *return_code*, **RACF RETURN CODE** *return_code*, **REASON CODE** *reason_code*.

Explanation: The RACF/DB2 external security module termination function for subsystem *subsystem-name* attempted to delete RACLISTed profiles for class *classname*. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

The attempt to delete the profiles using RACROUTE REQUEST=LIST,ENVIR=DELETE failed with the return and reason codes provided in the message text. The return and reason codes are in hexadecimal format.

System Action: The termination function continues processing. Resources are cleaned up when processing completes. This does not impact RACF authorization checking when DB2 is restarted.

Operator Response: Contact the DB2 system programmer.

System Programmer Response: Use the RACROUTE return code and the RACF return and reason codes to determine the cause of the failure.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR906I **RACF/DB2 TERMINATION FUNCTION COMPLETED WITH WARNINGS FOR DB2 SUBSYSTEM** *subsystem-name* **BECAUSE THE DEFAULT ACEE COULD NOT BE DELETED. RACROUTE RETURN CODE** *return_code*, **RACF RETURN CODE** *return_code*, **REASON CODE** *reason_code*.

Explanation: The RACF/DB2 external security module termination function for the subsystem *subsystem-name* attempted to delete the default ACEE used by the external security module. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

The attempt to delete the ACEE using RACROUTE REQUEST=VERIFY,ENVIR=DELETE failed with the return and reason codes provided in the message text. The return and reason codes are in hexadecimal format.

System Action: The termination function continues processing and resources are cleaned up when processing completes. This does not impact RACF authorization checking when DB2 is restarted.

Operator Response: Contact the DB2 system programmer.

System Programmer Response: Use the RACROUTE return code and the RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR907I **RACF/DB2 TERMINATION FUNCTION COMPLETED WITH WARNINGS FOR DB2 SUBSYSTEM** *subsystem-name* **BECAUSE THE INPUT ACEE WAS {MISSING | NOT VALID}.**

Explanation: The RACF/DB2 external security module termination function for the subsystem *subsystem-name* determined that the input DB2 subsystem ACEE was either not valid or missing. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

System Action: For exit termination, the RACF/DB2 external security module is not able to complete its termination function. This should not impact RACF authorization checking when DB2 is restarted.

Operator Response: Contact the DB2 system programmer.

System Programmer Response: Contact the IBM support center.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR908I **RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM** *subsystem-name* **HAS A MODULE VERSION OF** *module-version* **AND A MODULE LENGTH OF** *module-length*.

Explanation: The RACF/DB2 external security module initialization function for subsystem *subsystem-name* has determined the version and length of the RACF/DB2 external security module for subsystem *subsystem-name*. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem. *module-version* is the FMID or APAR number associated with the module. *module-length* is the hexadecimal length of all CSECTs contained in the module.

System Action: The RACF external security module continues.

Destination: Descriptor code is 4. Routing codes are 9 and 10.

IRR909I **RACF/DB2 EXTERNAL SECURITY
MODULE FOR DB2 SUBSYSTEM**
subsystem-name **IS USING OPTIONS:**
&CLASSOPT= *classopt* **&CLASSNMT=**
classnmt **&CHAROPT=** *charopt*
&ERROROPT= *erroropt* **&PCELLCT=**
pcellct **&SCELLCT=** *scellct*

Explanation: The RACF/DB2 external security module initialization function for subsystem *subsystem-name* lists the options that are being used for the RACF/DB2 external security module. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem. For an explanation of the options, see *z/OS Security Server RACF System Programmer's Guide*.

System Action: The RACF external security module continues.

Destination: Descriptor code is 4. Routing codes are 9 and 10.

IRR910I **RACF/DB2 EXTERNAL SECURITY
MODULE FOR DB2 SUBSYSTEM**
subsystem-name **INITIATED RACLIST
FOR CLASSES: {classname-list | ***
NONE *}

Explanation: The RACF/DB2 external security module initialization function for DB2 subsystem *subsystem-name* issued a RACROUTE REQUEST=LIST,GLOBAL=YES macro for classes *classname-list* as defined in the object table in the RACF/DB2 external security module. If **"* NONE *"** is displayed, an error occurred before the initialization function could issue RACROUTE REQUEST=LIST for any class. If this is DB2 data sharing, *subsystem-name* is the group attach name. Otherwise, it is the DB2 subsystem.

System Action: The RACF/DB2 external security module continues.

Destination: Descriptor code is 4. Routing codes are 9 and 10.

IRR911I **RACF/DB2 EXTERNAL SECURITY
MODULE FOR DB2 SUBSYSTEM**
subsystem-name **SUCCESSFULLY
RACLISTED CLASSES: {classname-list |**
*** NONE *}**

Explanation: The RACF/DB2 external security module initialization function for DB2 subsystem *subsystem-name* lists the classes for which the RACROUTE REQUEST=LIST,GLOBAL=YES macro was successful. If **"* NONE *"** is displayed, no classes were RACLISTed successfully. See message IRR910I to determine which classes the RACF/DB2 external security module attempted to use. The class list displayed in IRR911I might be a valid subset of the classes listed in message IRR910I. See *z/OS Security*

Server RACF Security Administrator's Guide for more information about initializing the RACF/DB2 external security module.

System Action: The RACF/DB2 external security module continues.

Destination: Descriptor code is 4. Routing codes are 9 and 10.

IRR912I **NATIVE DB2 AUTHORIZATION IS
USED.**

Explanation: RACF is not being used to control access to DB2 resources. This message is preceded by other messages that describe why RACF is not being used for access control decisions.

System Action: None. All subsequent access control decisions are made by DB2 using DB2's native security mechanism.

Operator Response: Follow the Operator Response for the message that preceded this message.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

IRR913I **DB2 SUBSYSTEM TERMINATION
REQUESTED.**

Explanation: RACF has requested that the DB2 subsystem be terminated. This message is preceded by another message which describes why this request has been made.

System Action: RACF has requested that the DB2 subsystem terminate.

Operator Response: Follow the Operator Response for the message that preceded this message.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

Chapter 6. IRR messages for commands, utilities, and other tasks

This section lists the messages with a prefix of IRR that can go to the user or the system operator. The format of these messages is:

IRRxxxxnnnt text

where:

IRR identifies the message as a RACF message.
xx identifies the function issuing the message.
nnn is the message serial number.
t is the type code (I = information, or A = action).
text is the text of the message.

The values for the *xx* field that identifies the function issuing the message are:

xx	Function or Utility
16	Messages common to several commands
52	Dynamic parse (IRRDPI00 command) messages
61	RACF cross-reference utility (IRRUT100)
62	RACF database verification utility (IRRUT200)
63	Block update command (BLKUPD)
65	RACF database split/merge utility (IRRUT400)
67	RACF SMF data unload utility (IRRADU00) and RACF database unload utility (IRRDBU00)
68	RACF remove ID utility (IRRRID00)
71	REXX RACVAR function
A0	RACF subsystem
B0	RACF subsystem
C0	RACF subsystem
D0	DISPLAY command messages
E0	SIGNOFF command messages
F0	RRSF send request handling task messages
G0	RRSF parmlib and initialization messages
H0	SET command messages
I0	RRSF handshaking messages
J0	RRSF connection local transaction program messages
K0	RACLINK command messages
L0	RACROUTE REQUEST=LIST messages
L1	CACHECLS profile messages
M0	TARGET command messages
N0	RRSF connection receive transaction program messages
O0	RRSF connection send transaction program messages
P0	RRSF messages
Q0	RRSF connection task messages
R0	RRSF output handling task messages
S0	RACLINK command messages
T0	RACLINK command or RRSF output handling task messages
U0	File allocation messages
V0	RRSF enveloping messages
X0	RACF operational modes and coupling facility related messages

Messages common to several commands

IRR16001I *command-name failed. profile-name is not a valid profile name for class class-name.*

Explanation: The profile name in the indicated command did not follow the format required for profiles in the indicated class.

System Action: Command processing stops.

User Response: Check the spelling and form of the profile name, and reissue the command.

IRR16002I *command-name failed. The file pool id is missing from profile name profile-name.*

Explanation: The profile name in the indicated command did not contain a file pool ID, which is required.

System Action: Command processing stops.

User Response: Check the spelling and form of the profile name, and reissue the command.

IRR16003I **WARNING for *command-name*. The existing internal profile *profile-name* is not valid and should be deleted.**

Explanation: The indicated profile name was found in the database, but it does not follow the format required for profiles in the class related to the indicated command.

System Action: In all cases, command processing continues with the next profile name.

User Response: Delete the invalid profile with the RDELETE command, or contact your system administrator to delete the profile.

Dynamic parse (IRRDPI00) messages

Dynamic parse messages can be issued at the following times:

- When dynamic parse is initialized
- When IRRDPI00 is run (usually during system IPL)
- When a user issues a RACF command that uses dynamic parse to check the syntax of the operands specified on the RACF command.

IRR52001I **Command IRRDPI00 is invalid when RACF is not active.**

Explanation: RACF is not active on the system. RACF must be active to issue the command.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report this message to your RACF security administrator.

Operator Response: Ensure that RACF is available, and IPL the system again.

IRR52002I **User *userid* not authorized to issue command IRRDPI00.**

Explanation: The user indicated in the message is not authorized to issue the IRRDPI00 command.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: See your RACF security administrator.

RACF Security Administrator Response: See *z/OS Security Server RACF System Programmer's Guide* for more information on using IRRDPI00.

IRR52003I **Command IRRDPI00 failed. Unable to establish ESTAE environment. Return code from ESTAE is *return-code***

Explanation: IRRDPI00 was unable to establish an error recovery environment. Processing cannot continue without such an environment.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Notify your system programmer.

System Programmer Response: See "Problem Determination."

Problem Determination: For a description of the ESTAE return code, see *z/OS MVS Programming: Authorized Assembler Services Reference ENF-IXG*.

IRR52004I **Command IRRDPI00 failed. Unable to process the parameters specified.**

Explanation: IRRDPI00 was unable process the parameters specified.

System Action: IRRDPI00 processing stops. No action is taken.

User Response: Reissue the IRRDPI00 utility with correct parameters. For a description of IRRDPI00, see

z/OS Security Server RACF System Programmer's Guide.

IRR52005I **Dynamic parse initialization failed. No action was taken. Return code from IKJPARS is *return-code***

Explanation: A call to the IKJPARS service routine failed with the indicated return code.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: See "Problem Determination."

Problem Determination: See *z/OS TSO/E Programming Services* for an explanation of the return code from the parse service routine.

IRR52006I **Unable to completely parse command *command* because the command line was incomplete. Processing continues with the next input line.**

Explanation: The parse service routine did not receive all the required operands, or an attention interrupt occurred before input was completed.

System Action: Processing continues with the next input line in the dynamic parse specifications data set.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52007I **Command IRRDPI00 failed. No action was taken. Return code from STACK is *return-code***

Explanation: An error occurred when the STACK service routine attempted to open the SYSUT1 data set.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: See "Problem Determination."

Problem Determination: See *z/OS TSO/E Programming Services* for an explanation of the return code from the STACK service routine.

IRR52008I **Command IRRDPI00 failed. No action was taken. Return code from GETLINE is *return-code***

Explanation: An error occurred when the GETLINE service routine attempted to read the SYSUT1 data set.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: See "Problem Determination."

Problem Determination: See *z/OS TSO/E Programming Services* for an explanation of the return code from the GETLINE service routine.

IRR52009I **Error in PUTLINE service routine. Processing continues with next input line. Return code is *return-code***

Explanation: An error occurred when the PUTLINE service routine attempted to echo a line of input.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: See "Problem Determination."

Problem Determination: See *z/OS TSO/E Programming Services* for an explanation of the return code from the PUTLINE service routine.

IRR52010I **Keyword *keyword* is specified out of order. Processing continues with next command.**

Explanation: The dynamic parse specifications commands were specified in the wrong order.

System Action: Processing continues with the next input line.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52011I **Name *name* is invalid. Possible line continuation problem. Processing continues with the next input line.**

Explanation: An invalid command was encountered in the input, or, if this is a valid keyword, a continuation character is missing on the previous input line.

System Action: Processing continues with the next input line.

IRR52012I • IRR52017I

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52012I Segment name invalid for profile type specified. Processing continues with the next command.

Explanation: The segment name specified for a PROFILE command is not correct for that profile type.

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Make sure that the level of the RACF database templates is compatible with the IRRDPSDS data set. Also, make sure that any updates to the templates that affected the IRRDPSDS data set were applied to the database via the IRRMIN00 PARM=UPDATE profile and that the system was IPLed to bring the correct templates into storage so the fields and segment names can be verified against those in IRRDPSDS.

IRR52013I Field name invalid for profile type specified.

Explanation: An invalid field name was specified on the KEYWORD command, or a RACF Data Base Template Field definition was not found for the field name specified.

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Make sure that the level of the RACF database templates is compatible with the IRRDPSDS data set. Also, make sure that any updates to the templates that affected the IRRDPSDS data set were applied to the database via the IRRMIN00 PARM=UPDATE profile and that the system was IPLed to bring the correct templates into storage so the fields and segment names can be verified against those in IRRDPSDS.

IRR52014I SUBFIELD keyword is invalid for flag field specifications. Processing continues with the next command.

Explanation: Flag field specifications require only the mask keywords ORMASK and ANDMASK to be specified. Information supplied by the SUBFIELD keyword does not pertain to flag field specifications.

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52015I Mask values are required for flag field specifications, but are not specified. Processing continues with the next command.

Explanation: Flag field specifications require the mask keywords ORMASK and ANDMASK to be specified. Information supplied by these commands is used to update the flag field in the RACF database.

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52016I SUBFIELD, TRANSLATE, and ANDMASK/ORMASK are mutually exclusive, only one may be specified. Processing continues with the next command.

Explanation: Explicit values are specified by the TRANSLATE keyword; therefore, no variable-value-subfield definition is required (in other words, the SUBFIELD keyword).

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52017I LIST keyword was not specified for a repeat group specification. Processing continues with the next command.

Explanation: The LIST keyword was specified and the RACF template definition showed the field named not to be a repeat group field.

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52018I **Length of ORMASK is too long for field in RACF data base. Processing continues with the next command.**

Explanation: The value of the mask was too large to fit in the amount of storage available for the field.

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52019I **Length of ANDMASK is too long for field in RACF data base. Processing continues with the next command.**

Explanation: The value of the mask was too large to fit in the amount of storage available for the field.

System Action: Processing continues with the next DPSDS command set.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52020I **Dynamic Parse storage allocation failed. No action taken. Return code is *return-code*. Internal code is *internal-code***

Explanation: The dynamic parse table was not installed.

System Action: Processing stops.

User Response: Contact system support.

System Programmer Response: Run IRRDPI00 (dynamic parse initialization program). For a description of IRRDPI00, see *z/OS Security Server RACF System Programmer's Guide*.

IRR52021I **You are not authorized to view *segment-name* segments.**

Explanation: The user requested to display segment information but did not have proper field-level access authority.

System Action: The requested segment information is not displayed for the requested profile(s). The base segment information is listed if the user is authorized and the NORACF keyword has not been specified.

RACF Security Administrator Response: For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

IRR52022I **Severe program error occurred. Consult your System Programmer. Internal code is *code***

Explanation: An error occurred in dynamic parse processing.

System Action: Processing stops.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Report the exact text of this message to your IBM support center.

IRR52023I **Invalid input to dynamic parse table update.**

Explanation: There is an error in the dynamic parse specifications data set.

System Action: Command processing stops.

User Response: Ensure that the correct dynamic parse specifications data set is specified.

IRR52024I **Unable to obtain space for Dynamic Parse Update work area. Return code from GETMAIN is *return-code***

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: For TSO users, log on with a larger region size. For MVS batch users, specify a larger region size for the job that failed.

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52025I **Unable to obtain space for Dynamic Parse Table. Return code from GETMAIN is *return-code*.**

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: For TSO users, log on with a larger region size. For MVS batch users, specify a larger ESCA size for the job that failed.

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52026I • IRR52101I

IRR52026I **Unable to FREEMAIN space for dynamic parse table. Size of FREEMAIN is *size* at location *location*. Return code is *return-code*.**

Explanation: Dynamic parse issued the FREEMAIN macro to release space, but the FREEMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Report the exact text of this message to your IBM support center.

IRR52027I **Unable to perform a check for this field against the RACF template definition because either PROFILE keyword information or SEGMENT keyword information was incomplete. Processing continues with the next command.**

Explanation: An error was encountered in the dynamic parse specifications data set.

System Action: Processing continues with the next input command.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52028I **Either PROMPT or DEFAULT must be specified for the SUBFIELD keyword. Processing continues with the next input command.**

Explanation: An error was encountered in the dynamic parse specifications data set.

System Action: Processing continues with the next input command.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52029I **PROMPT and DEFAULT are mutually exclusive, only one may be specified. Processing continues with the next input command.**

Explanation: An error was encountered in the dynamic parse specifications data set.

System Action: Processing continues with the next input command.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52030I **PTYPE must be specified when SUBFIELD is specified.**

Explanation: An error was encountered in the dynamic parse specifications data set.

System Action: Processing continues with the next input command.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52031I **Command IRRDPI00 failed because the dynamic parse specifications data set is empty. No action was taken.**

Explanation: There are no source statements in the dynamic parse specifications data set.

System Action: No action was taken.

User Response: Report this message to your system programmer.

System Programmer Response: Ensure the correct dynamic parse specifications data set is specified.

IRR52100I **Processing terminated. Dynamic parse is not active. Contact your system programmer.**

Explanation: An operand specified on a RACF command was not recognizable without dynamic parse.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report this message to your system programmer.

System Programmer Response: Ensure that IRRDPI00 was run during IPL and that the correct dynamic parse specifications data set was specified. See the *z/OS Security Server RACF System Programmer's Guide* for more information.

IRR52101I **Processing terminated. Unable to obtain storage for dynamic parse work area.**

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: For TSO users, log on with a larger

region size. For batch users, specify a larger region size for the job that failed.

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52102I Insufficient storage for internal work area. Processing terminated.

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52103I FREEMAIN failed for PCL work area. Contact your IBM support center.

Explanation: Dynamic parse issued the FREEMAIN macro to release space, but the FREEMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Report the exact text of this message to your IBM support center.

IRR52104I Dynamic parse exit *module-name* not found in load library. Command processing continues.

Explanation: The RACF dynamic parse exit indicated in the message was not found in the system LNKST concatenation.

System Action: Command processing continues without the function provided by the installation exit.

User Response: Report the exact text of this message to your system programmer. **Attention:** Some exits provide validation of the data you provided, while others may actually change the data from the external format you provided to an internal format suitable for use by the system. Neither the validation nor, if required, the data transformation occurred during execution of this RACF command because the command could not locate the exit. Therefore, the data you just placed into the segment may contain errors. You should have your system programmer install the needed exit and reissue the command so the exit can examine or modify the data.

System Programmer Response: Ensure that the indicated exit is in a library in the system LNKST concatenation.

IRR52105I Field in dynamic parse table is not found in template. Contact your system programmer.

Explanation: A keyword specified in the command is found in the dynamic parse table, but is not found in the associated template.

System Action: Command processing stops.

User Response: Report this message to your system programmer.

System Programmer Response: Check that the templates used for the RACF database are correct. If necessary, reinitialize RACF.

IRR52106I Segment not found in Template. Contact your system programmer.

Explanation: A segment name specified on the command is found in the dynamic parse tables, but is not found in the associated templates.

System Action: Command processing stops.

User Response: Report this message to your system programmer.

System Programmer Response: Check that the templates used for the RACF database are correct. If necessary, reinitialize RACF.

IRR52107I NOTIFY exit *module-name* not found.

Explanation: The installation exit indicated in the message was not found.

System Action: Command processing continues without the function provided by the installation exit.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Ensure that the indicated exit is in a LINKLIB or LPA library.

IRR52108I Insufficient storage for internal workarea. Processing terminated. GETMAIN return code is *return-code*. Internal code is *code*.

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

IRR52109I • IRR52117I

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52109I Dynamic parse storage allocation failed. No action taken. Return code is *return-code*.

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System Action: IRRDPI00 command processing stops. No action is taken.

User Response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52110I Insufficient storage for command buffer. Processing terminated.

Explanation: There is not enough storage for the command as issued.

System Action: Command processing stops.

User Response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52112I Sub-operands are not allowed with 'NO-' keyword. Processing terminated.

Explanation: A sub-operand that begins with NO cannot be specified.

System Action: Processing stops.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52113I Keyword *keyword* contains invalid or missing subfield(s). Processing continues.

Explanation: One or more subfields specified for the indicated keyword are incorrect or are required.

System Action: Processing stops.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52114I Processing terminated. Unable to obtain storage requested.

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System Action: IRRDPI00 command Processing stops. No action taken.

User Response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System Programmer Response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52115I Error during RACF manager processing. Return code is *return-code*. Reason code is *reason-code*.

Explanation: A RACF-manager error occurred during request processing.

System Action: Command processing stops.

User Response: Report the exact text of this message to your system programmer.

Problem Determination: Check the list of RACF-manager return codes in "RACF Manager Return Codes" on page 307. If the return code is listed, the explanation should help you investigate the problem. If the return code is not listed or relates to a problem with RACF (as opposed to a problem you can fix in the RACF database), report the complete text of this message to your IBM support center.

IRR52116I RACF data base access denied — RACF is not currently active or the RACF dataset containing the requested profile is not active.

Explanation: RACF is not active at the time of this request.

System Action: No action is taken.

User Response: Issue your request again. If the message persists, contact system support.

System Programmer Response: Check IPL processing to make sure that RACF is activated during system IPL.

IRR52117I LISTING exit *module-name* not found.

Explanation: The installation exit indicated in the message was not found.

System Action: Command processing continues without the function provided by the installation exit.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Ensure that the indicated exit is in a LINKLIB or LPA library.

IRR52118I Segment name abbreviation *value* is ambiguous. Please enter again.

Explanation: The segment name specified is not long enough.

System Action: If TSO prompting is on, the user is prompted for a valid segment name abbreviation. If TSO prompting is off, RACF command Processing stops.

User Response: Specify a longer segment name abbreviation.

IRR52119I Keyword name abbreviation *value* is ambiguous. Please enter again.

Explanation: The keyword name specified is not long enough.

System Action: If TSO prompting is on, the user is prompted for a valid keyword name abbreviation. If TSO prompting is off, RACF command Processing stops.

User Response: Specify a longer keyword name abbreviation.

IRR52120I SIZE *size* is out of range.

Explanation: The region size specified is incorrect for your system.

System Action: If TSO prompting is on, the user is prompted for a valid keyword name abbreviation. If TSO prompting is off, RACF command Processing stops.

User Response: The region size specified is probably too large. If so, specify a smaller region size.

IRR52121I SIZE specified is greater than MAXSIZE. SIZE is adjusted to be equal to MAXSIZE.

Explanation: The value specified for SIZE cannot be greater than the value specified for MAXSIZE.

System Action: RACF adds a user profile, but adjusts SIZE to equal the MAXSIZE operand.

User Response: To change the SIZE or MAXSIZE operands for this user profile, use the ALTUSER command.

IRR52122I Conflict between SIZE and MAXSIZE. Operand ignored.

Explanation: The values specified on the SIZE and MAXSIZE operands are incompatible.

System Action: RACF adds a user profile, but ignores the SIZE and MAXSIZE operands.

User Response: To change the SIZE or MAXSIZE

operands for this user profile, use the ALTUSER command.

IRR52123I Data must be hexadecimal.

Explanation: The data specified can be A through Z or 0 through 9.

System Action: Command processing stops.

User Response: Correct the data and issue the command again.

IRR52124I Operand is not valid. Session key interval is not in range 1 - *value*.

Explanation: The session key change interval specified for a session segment must be greater than or equal to 1 and less than or equal to *value*, where *value* varies according to the setting of SETROPTS SESSIONINTERVAL. If SETROPTS SESSIONINTERVAL is in effect, or defaulted, then *value* is the SESSIONINTERVAL value. If SETROPTS NOSESSIONINTERVAL is in effect, then the value is 32767.

System Action: If you are in prompt mode (on TSO, PROFILE PROMPT is in effect), you receive a prompt to reenter the operand. If you are not in prompt mode, command processing stops.

User Response: Specify a valid value for the INTERVAL operand, by either responding to the prompt, or by reentering the command.

IRR52125I Operand is not valid. Session key exceeds 8 characters.

Explanation: The user has entered more than eight characters of character data for a session key. The maximum length is eight characters.

System Action: If you are in prompt mode (on TSO, PROFILE PROMPT is in effect), you receive a prompt to reenter the operand. If you are not in prompt mode, command processing stops.

User Response: Specify a valid value for the SESSKEY operand, either by responding to the prompt, or by reentering the command.

IRR52126I RACXTRT failed. Return code is *return-code*. Reason code is *reason-code*.

Explanation: RACROUTE REQUEST=EXTRACT failed because of an error in an installation exit, or because of an internal error.

System Action: Command processing stops.

User Response: See your RACF administrator.

Problem Determination: See the description of return and reason codes for the REQUEST=EXTRACT macro

IRR52127I • IRR52133I

in *z/OS Security Server RACROUTE Macro Reference*.
Check any related installation exit for a possible error.

IRR52127I Field level access checking failed for segment *segment-name*.

Explanation: You do not have authorization to the indicated segment.

System Action: Command processing stops.

User Response: Report the exact text of this message to your RACF security administrator.

RACF Security Administrator Response: For a description of field-level access checking, see *z/OS Security Server RACF Security Administrator's Guide*.

IRR52128I Mutually exclusive operands are specified for keyword *keyword*. Processing terminated.

Explanation: One or more pairs of operands cannot be specified together on the indicated keyword in the dynamic parse specifications data set.

System Action: Processing stops.

User Response: Report this message to your system programmer.

System Programmer Response: Report this message to your IBM support center.

IRR52129I The PRIMARY sub-operand was ignored. *value* is not a valid language code.

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM.

System Action: The user's default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile is created.

User Response: Issue the ALTUSER command with a valid language code specified.

IRR52130I The PRIMARY sub-operand was ignored. The MVS message service is not active.

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained because the MVS message service is not active.

System Action: The user's default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were

issued by RACF, the user profile was created.

User Response: Issue the ALTUSER command with a valid language code specified.

IRR52131I The PRIMARY sub-operand was ignored. The specified language is not active.

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained from the MVS message service.

System Action: The user's default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

User Response: Issue the ALTUSER command with a valid language code or language name specified.

IRR52132I The SECONDARY sub-operand was ignored. *value* is not a valid language code.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM.

System Action: The user's default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

User Response: Issue the ALTUSER command with a valid language code specified.

IRR52133I The SECONDARY sub-operand was ignored. The MVS message service is not active.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained because the MVS message service is not active.

System Action: The user's default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

User Response: Issue the ALTUSER command with a valid language code specified.

IRR52134I The SECONDARY sub-operand was ignored. The specified language is not active.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code could not be obtained from the MVS message service.

System Action: The user's default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

User Response: Issue the ALTUSER command with a valid language code or language name specified.

IRR52135I The PRIMARY sub-operand was ignored. QRYLANG macro failed with return code xxxx and reason code yyyy.

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was therefore assumed to be an installation-defined language name, but the required language code could not be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyyy.

System Action: The user's default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

User Response: Report the complete text of this message to your system programmer.

System Programmer Response: See *z/OS MVS Programming: Authorized Assembler Services Reference LLA-SDU* for a description of return codes and reason codes for the QRYLANG macro.

IRR52136I The SECONDARY sub-operand was ignored. QRYLANG macro failed with return code xxxx and reason code yyyy.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was therefore assumed to be an installation-defined language name, but the required language code could not be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyyy.

System Action: The user's default for the

SECONDARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

User Response: Report the complete text of this message to your system programmer.

System Programmer Response: See *z/OS MVS Programming: Authorized Assembler Services Reference LLA-SDU* for a description of return codes and reason codes for the QRYLANG macro.

IRR52137I Purge of VLF class IRRUMAP failed with return code nn

Explanation: Dynamic parse attempted to purge a VLF entry in the UID-to-user ID mapping table because a change was made to UID information by an ALTUSER or DELUSER command. The module called to purge the entry, IRRMAP00, returned an unexpected return code.

System Action: Command processing successfully updates the user profile, but the in-storage information that maps the user ID to a UID may not match the information on the RACF database.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Report the exact text of this message to your IBM support center. The following decimal return codes may appear in the message. They indicate an unexpected error in the command's processing or the user's TSO environment:

Code	Explanation
8	Object not found in VLF
12	No ACEE available
16	VLF failure
20	ACEE is not version 2
999	Parameter list error

IRR52138I Purge of VLF class IRRGMAP failed with return code nn

Explanation: Dynamic parse attempted to purge a VLF entry in the GID-to-group name table because a change was made to GID information by an ALTGROUP or DELGROUP command. The module called to purge the entry, IRRMAP00, returned an unexpected return code.

System Action: Command processing successfully updates the group profile, but the in-storage information that maps the group name to a GID may not match the information on the RACF database.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Report the exact text of this message to your IBM support center. The following decimal return codes may appear in the

IRR52139I • IRR52145I

message. They indicate an unexpected error in the command's processing or the user's TSO environment:

Code	Explanation
8	Object not found in VLF
12	No ACEE available
16	VLF failure
20	ACEE is not version 2
999	Parameter list error

IRR52139I **KEYMASKED or KEYENCRYPTED data must be 16 hexadecimal characters.**

Explanation: You entered data in the KEYMASKED or KEYENCRYPTED suboperand that:

- Is not exactly 16 characters long.
- Contains characters other than the hexadecimal characters 0 through 9 and A through F.

System Action: If TSO prompting is active for the session, TSO prompts you to re-enter the suboperand. If TSO prompting is not active, command processing stops.

User Response: Reenter the suboperand correctly. Be sure it is 16 characters long and contains only characters 0 through 9 and A through F.

IRR52140I **Either the KEYMASKED or the KEYENCRYPTED sub-operand has been specified twice. Command Processing stops.**

Explanation: You entered the KEYMASKED or KEYENCRYPTED suboperand twice. The suboperand can be specified only once.

System Action: Command processing stops.

User Response: Reenter the command and specify the KEYMASKED or KEYENCRYPTED suboperand only once.

IRR52141I **KEYMASKED and KEYENCRYPTED are mutually exclusive sub-operands, and both have been specified. Command Processing stops.**

Explanation: You specified both the KEYMASKED and the KEYENCRYPTED suboperands, which are mutually exclusive. You can specify only one operand at a time.

System Action: Command processing stops.

User Response: Reenter the command with either the KEYMASKED or the KEYENCRYPTED suboperand.

IRR52142I **The KEYENCRYPTED sub-operand was specified but a Cryptographic product is not available on this system. Command Processing stops.**

Explanation: The KEYENCRYPTED suboperand is not available. A cryptographic product is not available on this system.

System Action: Command processing stops.

User Response: Reenter the command with the KEYMASKED suboperand if you want to mask the secured signon key when it is stored on the RACF database.

IRR52143I **Warning: =MEMBER should not be specified for both USER and GROUP.**

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment, and the resulting STDATA information in the RACF database specifies the value =MEMBER for both the user ID and the group name. This is an incorrect configuration. The member name can be valid as a user ID or a group name, but not both.

System Action: If the profile is not corrected before it is used to process an MVS START command, RACF uses the =MEMBER value for the user ID and blanks (signifying the assigned user's default group) as the group name.

User Response: Use the RALTER command to assign a different value for either USER or GROUP.

IRR52144I **Warning: User *userid* is not defined to RACF.**

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment, and the *userid* specified in the USER field does not exist in the RACF database.

System Action: If the profile is not corrected before it is used to process an MVS START command, RACF assigns the indicated *userid* to the procedure or job being started.

User Response: Use the RALTER command to assign the correct *userid* for USER, or use the ADDUSER command to define the user to RACF.

IRR52145I **Warning: Group *group-name* is not defined to RACF.**

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment, and the *group-name* specified in the GROUP field does not exist in the RACF database.

System Action: If the profile is not corrected before it is used to process an MVS START command, RACF

assigns the indicated *group-name* to the procedure or job being started.

User Response: Use the RALTER command to assign the correct *group-name* for GROUP, or use the ADDGROUP command to define the group to RACF.

IRR52146I Warning: User *userid* is not connected to group *group-name*.

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment, but the *userid* specified in the USER field is not connected to the *group-name* specified in the GROUP field.

System Action: If the profile is not corrected before it is used to process an MVS START command, RACF assigns the indicated *userid* to the procedure or job being started.

User Response: Use the RALTER command to assign the correct *userid* or *group-name* for USER or GROUP, or use the CONNECT command to connect the user to the group.

IRR52147I Note: Specification of a value for GROUP is recommended for this profile.

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment. The *profile_name* contains generic characters in the portion of the name that would match the member name for a START command, and the USER value is “=MEMBER”. Also, there is no value for GROUP.

As documented in *z/OS Security Server RACF Security Administrator's Guide*, this is a dangerous configuration because a new started procedure or job could be created that would match an existing user ID.

System Action: The data in the STDATA segment is used if an appropriate MVS START command is issued. The member name is assigned as the user ID and the user's default group is used.

User Response: If you have a special group for started procedure or job user IDs, use the RALTER command to specify the GROUP value. If you do not have such a group, consider defining one and assigning it via the RALTER command to avoid potential problems with started procedure or job user IDs accidentally matching the user IDs of other users on your system.

IRR52148I Warning: A value for USER should be specified in STDATA.

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment, and no value has been specified for the USER field.

System Action: If the profile is not corrected before it is used to process an MVS START command, RACF uses information from the started procedure table (ICHRIN03) instead.

User Response: Use the RALTER command to specify a value for USER.

IRR52149I Warning: STARTED profiles should have (or match) names with two qualifiers.

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment, and the *profile_name* does not appear to have the correct number of qualifiers to be useful. The *profile_name* specified on the RDEFINE or the RALTER command appears to have only one qualifier, or more than two, and thus is not used to process START commands.

Note: All STARTED resource names are of the format *memname.jobname*(or *memname.memname* if no *jobname* is specified on the MVS START command). However, there are some cases where the profile may have only one qualifier or three qualifiers and still work. For example:

- If the STARTED profile name is &X, and the &X profile in RACFVARS is defined as “RDEFINE RACFVARS &X ADDMEM(A.A)”, the profile would be used when starting procedure A with no job name.
- A profile name of the form *.*.* (or several other unlikely generic combinations) could be used to match names with two qualifiers.

System Action: Except for the cases noted in the explanation, the profile is not used to process MVS START commands.

User Response: Unless the *profile_name* matches one of the exception cases noted in the explanation, you should delete the profile using the RDELETE command and then use the RDEFINE command to define a profile with the correct name.

IRR52150I Warning: SETROPTS GENERIC(STARTED) should have been issued before defining this profile.

Explanation: This message is issued when the RDEFINE or the RALTER command specifies the STDATA segment. The profile name contains generic characters (*, %, or &), but the STARTED class has not been specified as a generic class.

System Action: The profile is not used to process MVS START commands.

User Response:

1. Use the RDELETE command to delete the profile; then

IRR52151I • IRR52153I

2. Issue SETROPTS GENERIC(STARTED), or have someone with RACF SPECIAL issue it; then
3. Use the RDEFINE command to create the profile again.

IRR52151I Unexpected RACROUTE REQUEST=EXTRACT error while retrieving profile. SAF RC = *safrc*, RACF RC = *racrc*, RACF RSN = *rsncode*.

Explanation: This message gives the resulting SAF return code, a RACF return code (SAFPRRET), and a RACF reason code (SAFPRREA). If the value of a return code or reason code is greater than X'0000FFFF', it is displayed as a hexadecimal number. If the value is less than or equal to X'0000FFFF', it is displayed as a decimal number.

This message can be issued in three situations:

- If the message indicates a USER, GROUP, CONNECT, or STARTED profile, the message is issued when an RDEFINE or RALTER command specifies the STDATA segment. An unexpected error occurred from a RACROUTE REQUEST=EXTRACT macro that was used to retrieve information for the STDATA segment.
- If you modified DCE, OMVS, or OVM information in a user profile, the DCE, OMVS, or the OVM segment of the RACF profile changed but the corresponding update in the DCEUIDS, UNIXMAP, or VMPOSIX class for the user or group profile did not occur. RACF attempted to retrieve the information from the profile specified in the message text but has encountered an error.
- If you modified LNOTES, NDS, or KERB information in a USER profile, the LNOTES, NDS, or KERB segment of the profile changed but the corresponding NOTELINK, NDSLINK, or KERBLINK mapping class profile was not updated. RACF attempted to retrieve the LNOTES, NDS, or KERB information from the profile specified in the message text but has encountered an error.

System Action: Command processing continues in a specific way for each of the following:

- If the message indicates a USER, GROUP, CONNECT, or STARTED profile, processing of the RDEFINE or RALTER command completed successfully. Data specified for the STDATA segment was processed, along with any other data on the command.
- If you were modifying DCE, OMVS, or OVM information in a user profile, command processing continues. However, the mapping profiles in the DCEUIDS, UNIXMAP, or VMPOSIX class are not updated.
- If you were modifying LNOTES, NDS, or KERB information in a user profile, command processing

continues. However, the mapping profiles in the NOTELINK, NDSLINK, or KERBLINK class are not updated.

User Response: Report this message to the system programmer and provide the exact text of the command you issued.

System Programmer Response: Use the return code information in *z/OS Security Server RACROUTE Macro Reference* to determine the error condition and fix the error. If necessary, contact the IBM support center. Tell them the command issued and the resulting return and reason codes.

- If you were updating DCE, OMVS, or OVM information and you have corrected the error, reissue the command. As an alternative, use the RACF RALTER or RDELETE command to manually administer the DCEUIDS, UNIXMAP, or VMPOSIX class profile that corresponds to the user profile you were changing.
- If you were updating OMVS or OVM information in user or group profiles, you can use the RACF RDEFINE or PERMIT command to manually update the access list of the appropriate UNIXMAP or VMPOSIX class profile.
- If you were updating LNOTES, NDS, or KERB information and you have corrected the error, reissue the command. As an alternative, try to delete the information and add it again. If the SNAME, UNAME, or KERBNAME values are in upper case characters, use the RACF RALTER or RDELETE command to manually administer the NOTELINK, NDSLINK, or KERBLINK class profile that corresponds to the user profile you were changing. For details on the mapping profiles, see *z/OS Security Server RACF Security Administrator's Guide*.

IRR52152I Both AT and ONLYAT cannot be specified for the same command. The command is not issued.

Explanation: The AT and ONLYAT keywords are mutually exclusive. Only one may be specified.

System Action: Command processing ends.

User Response: Issue the command again, specifying either the AT or ONLYAT keyword, but not both.

IRR52153I Unexpected return code *return-code* and reason code *reason-code* encountered while attempting an ICHEINTY operation.

Explanation: An ICHEINTY macro was issued to update the RACF database but returned an unexpected return and reason code. The error occurred when RACF attempted to update one of the following:

- A UUID-to-user ID mapping profile because an ADDUSER, ALTUSER, or DELUSER command changed the DCE UUID information.

- A UNIXMAP class mapping profile because an ADDUSER, ALTUSER, DELUSER, ADDGROUP, ALTGROUP, or DELGROUP command changed an OMVS UID or OMVS GID
- A VMPOSIX class mapping profile because an ADDUSER, ALTUSER, DELUSER, ADDGROUP, ALTGROUP, or DELGROUP command changed an OVM UID or OVM GID
- A NOTELINK, NDSLINK, or KERBLINK mapping profile because an ADDUSER, ALTUSER, or DELUSER command changed an LNOTES SNAME, an NDS UNAME, or KERB KERBNAME.

Return code *return-code* and reason code *reason-code* are displayed in decimal. Message IRR52154I follows this message immediately and identifies the mapping profile that was being changed.

System Action: The profile is updated according to each of the following circumstances:

- If you are modifying DCE UUIDs contained in RACF user profiles, command processing updates the user profile successfully. However, the mapping profile in the DCEUUIDS class that maps the DCEUUID to a RACF user ID might not match the information in the user profile.
- If you are modifying OMVS information in user or group profiles (UID or GID), command processing updates the profile successfully. However, the mapping profile in the UNIXMAP class that maps an OMVS UID or OMVS GID to a RACF user or group might not match the information in the corresponding profile.
- If you are modifying OVM information in user or group profiles (UID or GID), command processing updates the profile successfully. However, the mapping profile in the VMPOSIX class that maps a POSIX UID or POSIX GID to a RACF user or group might not match the information in the corresponding profile.
- If you are modifying LNOTES or NDS information in a user profile (SNAME or UNAME), command processing updates the profile successfully. However, the mapping profile in the NOTELINK or NDSLINK class that maps an LNOTES SNAME or NDS UNAME to a RACF user might not match the information in the corresponding profile. See message IRR52154I for information describing the mismatch.

System Programmer Response: If the problem occurred with the NOTELINK, NDSLINK, or KERBLINK profiles, see message IRR52154I for the steps you need to follow to correct the error.

Report the exact text of this message to the IBM support center. For details on the mapping profiles, see *z/OS Security Server RACF Security Administrator's Guide*.

User Response: Report the exact text of this

message to your system programmer.

IRR52154I The information in the *class1* mapping profile *profile1* does not match the *profile2* profile in the *class2* class.

Explanation: This message, which follows IRR52153I, identifies the mapping profile that was being changed when the error described in IRR52153I occurred. See that message for further information.

System Action: The user or group profile specified in the RACF command was updated successfully. However, the DCEUUIDS, NOTELINK, NDSLINK, VMPOSIX, or KERBLINK mapping profiles were not updated. See IRR52153I for a detailed explanation.

System Programmer Response: If the problem occurred with the NOTELINK, NDSLINK, or KERBLINK profiles, perform the following steps:

1. Determine the first user ID that was assigned this application user name.
 - If the application user name contains lower case letters, use the RLIST NOTELINK *, RLIST NDSLINK *, or RLIST KERBLINK * command in the background to display the user ID in the Application Data field of the resource profile for the NOTELINK, NDSLINK, or KERBLINK class.
 - If the application user name contains only upper case letters, issue the RLIST NOTELINK *profile-name*, RLIST NDSLINK *profile-name*, or RLIST KERBLINK *profile-name* command, using the terminal monitoring program (TMP). You can find the user ID in the application data field.
2. If the Application Data field contains the user ID which should be associated with this LNOTES SNAME, NDS UNAME, or KERB KERBNAME, then no further problem determination or corrective actions are necessary. The IRR52153I message indicates that a residual NOTELINK, NDSLINK, or KERBLINK profile was found. However, the information in the profile is correct.
3. If the Application Data field does not contain the user ID which should be associated with this LNOTES SNAME, NDS UNAME, or KERB KERBNAME, then issue an ALTUSER command with the NOLNOTES, NONDS, or NOKERB operand for that user ID.
4. Select a new LNOTES SNAME, NDS UNAME, or KERB KERBNAME for this user ID and issue a new ALTUSER command to associate this user ID with the new SNAME, UNAME, or KERBNAME.
5. Issue the ALTUSER command again for the original user ID and specify the user's original SNAME, UNAME, or KERBNAME. This recreates the original user's identity mapping profile that was deleted in step 3.

If the problem occurred with any of the other mapping profiles, report the exact text of this message to the IBM

IRR52155I • IRR52160I

support center. For details on the mapping profiles, see *z/OS Security Server RACF Security Administrator's Guide*.

IRR52155I **The DCE principal UUID must be unique for each RACF User ID. The DCEUUIDS mapping profile is not updated.**

Explanation: RACF has detected that an ADDUSER or ALTUSER command tried to assign a principal UUID to more than one RACF user. Although the ADDUSER or ALTUSER command can complete successfully, a corresponding update is *not* made in the DCEUUIDS class.

System Action: The DCE segments of the user profiles specified on the command line are updated. However, the appropriate DCEUUIDS class profile for each user does not change.

User Response: Determine the correct principal UUID as listed in the DCE registry for this RACF/DCE user. Reissue the ALTUSER command to set the principal UUID in the RACF DCE segment to the UUID listed in the DCE registry.

IRR52156I **Purge of VLF class IRRSMAP failed with return code *return-code*.**

Explanation: RACF attempted to purge a VLF entry in the user ID-to-USP mapping table because z/OS UNIX System Services information was changed by an ALTUSER, DELUSER, or ALTGROUPO command. The module called to purge the entry, IRRMAP00, returned an unexpected return code.

System Action: Command processing successfully updates the user or group profile, but the in-storage information that maps a user ID to a USP may not match the information in the RACF database.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Report the exact text of this message to the IBM support center. The following decimal return codes may appear in the message. They indicate an error in the command's processing or the user's TSO environment:

Code	Explanation
8	Object not found in VLF
12	No ACEE available
16	VLF failure
20	ACEE is not version 2
999	Parameter list error

IRR52157I **Field *field-name* is not allowed for a profile in class *class-name*.**

Explanation: An attempt was made to define a field that is not allowed for a profile in the indicated class.

System Action: Command processing ends.

User Response: Decide whether the field name or class name was in error and issue a corrected command if necessary.

System Programmer Response: If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52158I **Field *field-name* exceeds *limit* characters.**

Explanation: The value specified for the field is too long. The maximum length is *limit*.

System Action: Command processing ends.

User Response: Retry the command specifying a shorter field value.

System Programmer Response: If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52159I **Required subfield *subfield-name* in field *field* is not specified.**

Explanation: A required subfield of a field specification is missing.

System Action: Command processing ends.

User Response: Include the indicated subfield and retry the command.

System Programmer Response: If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52160I **Subfield *subfield-name* in field *field* is not valid.**

Explanation: An incorrect value was identified for the indicated subfield.

- For conditional access authority, the value must be NONE, EXECUTE, READ, UPDATE, CONTROL, or ALTER.
- For a conditional access class, the value must be APPCPORT, CONSOLE, JESINPUT, PROGRAM, TERMINAL, or SYSID.

System Action: Command processing ends.

User Response: Retry the command specifying a valid value for the subfield.

System Programmer Response: If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52161I The application user identity must be unique for each RACF User ID. The mapping profile for *userid* will not be not updated.

Explanation: An ADDUSER or ALTUSER command tried to assign the same Lotus Notes for z/OS short name or Novell Directory Services user name to more than one RACF user. Although the command can complete successfully, a corresponding update is not made in the corresponding NOTELINK or NDSLINK mapping class.

System Action: The LNOTES or NDS segment of the user profile specified by the command is updated. However, the appropriate NOTELINK or NDSLINK class profile for each user does not change.

User Response: To correct the problem, perform the following steps:

1. Determine the first user ID that was assigned this application user name.
 - If the application user name contains lower case letters, use the RLIST NOTELINK * or RLIST NDSLINK * command in the background to display the user ID in the application data field of the resource profile for the NOTELINK or NDSLINK class.
 - If the application user name contains only upper case letters, issue the RLIST NOTELINK *profile-name* or RLIST NDSLINK *profile-name* command, using the terminal monitoring program (TMP). You can find the user ID in the application data field.
2. Issue an ALTUSER command with the NOLNOTES or NONDS operand for that user ID.
3. Select a new short name for user *userid* and issue a new ALTUSER command to associate this user ID with a new short name or user name.
4. Issue the ALTUSER command again for the original user ID and specify the user's original short name or user name. This recreates the original user's identity mapping profile that was deleted in step 2.

IRR52162I Unable to determine the name of the local Kerberos realm. Command processing ends.

Explanation: An ADDUSER KERB (KERBNAME) or ALTUSER KERB (KERBNAME) command was issued, but the local Kerberos realm is not defined to RACF. The local Kerberos realm must be defined to RACF before a local Kerberos principal name can be defined.

System Action: Command processing ends.

User Response: If the KERBDFTL REALM class profile is not defined, use RDEFINE to define the KERBDFTL profile in the REALM class and supply the KERBNAME operand to define the name of the local Kerberos realm. If the KERBDFTL REALM class profile

is already defined, specify the KERBNAME operand on a RALTER command to define the name of the local Kerberos realm.

IRR52163I The "char" character is not allowed in KERBNAME. Command processing ends.

Explanation: The name specified using the KERBNAME operand contains the character "char", which is not allowed. A local Kerberos principal name (defined by the ADDUSER or ALTUSER command) must not include the "@" character; a local Kerberos realm name (defined by the RDEFINE or RALTER command) must not contain the "/" character.

System Action: Command processing ends.

User Response: Reissue the command specifying a valid KERBNAME.

IRR52164I KERBNAME may not be prefixed by "/.../". Command processing ends.

Explanation: RACF uses a convention of "/.../realm_name/principal_name" to represent fully qualified Kerberos foreign principal names. Local Kerberos principal names, however, may not be fully qualified when specified on an ADDUSER or ALTUSER command. A KERBNAME which begins with the string "/.../" would be interpreted as a fully qualified name, so the prefix is not allowed.

System Action: Command processing ends.

User Response: Reissue the command specifying a valid KERBNAME.

IRR52165I The value for the *segment_name* segment operand must be unique. Command processing ends.

Explanation: The application identity name assigned for the *segment_name* segment by the ADDUSER or ALTUSER command is already assigned to another RACF user. The same application identity name cannot be assigned to more than one user. If a list of users had been specified in the command, the command fails because the same application identity name would have been assigned to each user in the list.

System Action: Command processing ends.

User Response: Reissue the command, specifying a unique name in the *operand_name* operand.

IRR52166I The fully qualified form of the local Kerberos principal name must not exceed 240 characters. Command processing ends.

Explanation: The length of the fully qualified form of the local Kerberos principal name

IRR52167I • IRR52172I

(/.../local_realm_name/local_principal_name) exceeds the limit of 240 characters.

System Action: Command processing ends.

User Response: Use the RLIST command to determine the name of the local Kerberos realm, then reissue the ADDUSER or ALTUSER command, specifying a local Kerberos principal name which will not exceed the 240 character limit in its fully qualified form.

IRR52167I Unable to validate MINTKTLFE, MAXTKTLFE, and DEFTKTLFE. Ticket lifetime values are ignored.

Explanation: Specified values for ticket lifetime (MINTKTLFE, MAXTKTLFE, or DEFTKTLFE) cannot be validated and will be ignored. Validation requires all three ticket lifetime values. However, one or more ticket lifetime values cannot be determined.

System Action: Ticket lifetime values are ignored.

User Response: Determine which ticket lifetime values are required and reissue the command using the following guidelines:

- For the RDEFINE command, all three ticket lifetime values (MINTKTLFE, MAXTKTLFE, and DEFTKTLFE) must be specified together on the same command.
- For the RALTER command, if the ticket lifetime values are being initially defined, all three values (MINTKTLFE, MAXTKTLFE, and DEFTKTLFE) must be specified together on the same command.
- For the RALTER command, if previously defined ticket lifetime values are being changed, any undefined values (MINTKTLFE, MAXTKTLFE, or DEFTKTLFE) must be specified together on the same command.

If ticket lifetime values have been previously defined for this local Kerberos realm, the RALTER command may be used to alter one or more of them, but if any one of them has been deleted by means of the NOMINTKTLFE, NOMAXTKTLFE, or NODEFTKTLFE operand, this ticket lifetime value is no longer defined and must be included on the same RALTER command. Use the RLIST command to determine undefined values.

IRR52168I Values specified for MINTKTLFE, MAXTKTLFE, or DEFTKTLFE are not valid. Ticket lifetime values are ignored.

Explanation: The ticket lifetime values are not consistent with each other. The value of MINTKTLFE must be less than the value of MAXTKTLFE and the value of DEFTKTLFE must be greater than the value of MINTKTLFE and less than the value of MAXTKTLFE.

System Action: Ticket lifetime values are ignored.

User Response: Use the RLIST command to

determine the current ticket lifetime values, if any. Reissue the command, specifying valid values for MINTKTLFE, MAXTKTLFE, or DEFTKTLFE.

IRR52169I A request to process Kerberos key information for *profile-name* failed. Command processing continues.

Explanation: An error occurred while attempting to generate a Kerberos key for the user or REALM class profile that is having its password changed through the use of the ALTUSER, RDEFINE, or RALTER command.

System Action: All processing except for the key update is completed.

User Response: Use the RLIST command to list the KERBDFLT profile definition of the local Kerberos realm in the REALM class and verify that the local realm name (KERBNAME) is defined. Use the appropriate list command (LISTUSER, RLIST) to list the KERB segment information for this user or REALM class and verify that this information may be accessed. Correct any problems and reissue the command.

IRR52170I The LDAP URL specified by the LDAPHOST operand was not prefixed by "ldap://" or "ldaps://". Command processing ends.

Explanation: An LDAP URL must start with either ldap:// or ldaps://, such as ldap://123.45.6:389 or ldaps://123.45.6:636.

System Action: Command processing ends.

User Response: Reissue the command, specifying an LDAP URL with the appropriate ldap:// or ldaps:// prefix.

IRR52171I Password not valid for LDAP BIND. Command processing ends.

Explanation: The specified password is not valid for LDAP BIND. For example, it should not start with the '{' character (hexadecimal x'8B').

System Action: Command processing ends.

User Response: Reissue the command, specifying a password which is valid for LDAP BIND.

IRR52172I A request to process LDAP BIND password information for *profile-name* failed. Command processing continues.

Explanation: An error occurred while attempting to mask or encrypt the LDAP BIND password which was specified for the user or FACILITY class profile PROXY segment through the use of the ADDUSER, ALTUSER, RDEFINE, or RALTER command.

System Action: All processing except for the LDAP BIND password update is complete. The LDAP BIND

password has not been added to the user or FACILITY class profile PROXY segment.

User Response: Use the SETROPTS command to determine if the KEYSMSTR class is activated. Use the RLST command to determine that the KEYSMSTR class LDAP.BINDPW.KEY profile has been defined and that it has a SSIGNON segment that contains either a masked or encrypted key. If key encryption is requested, determine that a cryptographic product is present on the system and that it is active. The cryptographic product must be active when you define the profile to the KEYSMSTR class. Correct any problems and reissue the command.

IRR52173I RACF was unable to determine if additional application password processing is required. Command processing continues.

Explanation: A TSO parse error prevented RACF from determining if the command contains an application password which requires additional processing, such as:

- Generation of a Kerberos key
- Encryption or masking of an LDAP BIND password

System Action: All processing except for the additional application password processing is completed.

- If the command specified a password which should be used to generate a Kerberos key, the key was not generated and not stored in the RACF profile.
- If the command specified an LDAP BIND password, the password was not encrypted or masked and not stored in the RACF profile.

User Response: Report this message and any related TSO parse messages to the system programmer and provide the exact text of the command issued.

System Programmer Response: Correct any reported TSO parse problems and ask the user to reissue the command. If this does not correct the problem, report this message to the IBM support center and provide the exact text of the command issued.

IRR52174I Incorrect [UID|GID] id. This value is already in use by name.

Explanation: You tried to assign a user a UID value which is already in use, or you tried to assign a group a GID which is already in use. The user or group is identified by *name*. Note that it is possible that more than one user or group is currently using the value, but only one of them is identified, and that one is arbitrarily chosen. If you wish to see a complete list, issue SEARCH CLASS(USER) UID(*id*) or SEARCH CLASS(GROUP) GID(*id*).

System Action: Command processing stops.

RACF Security Administrator Response:

If the command issuer should be allowed to assign shared UIDs and GIDs, then permit the user with READ access to the resource named SHARED.IDS in the UNIXPRIV class. The user should then reissue the command using the SHARED keyword.

User Response: Do one of the following:

1. Choose another value for *id* and issue SEARCH CLASS(USER) UID(*id*) or SEARCH CLASS(GROUP) GID(*id*) to make sure the new value is not also in use. Then, reissue the original command with the new value for *id*.
2. Let RACF choose an unused value for you by reissuing the command with the AUTOUID or AUTOGID keyword. For example: ADDUSER JORDAN OMVS(AUTOUID)
3. Reissue the command with the SHARED keyword to force RACF to assign the *id* despite it already being in use. The SHARED keyword requires the SPECIAL attribute or READ authority to the SHARED.IDS resource in the UNIXPRIV class.

IRR52175I You are not authorized to specify the SHARED keyword.

Explanation: You are attempting to specify the SHARED keyword to assign a UID or GID value which is already in use. You have not been authorized for this action.

System Action: Command processing stops.

RACF Security Administrator Response:

If appropriate, permit the user with READ access to the SHARED.IDS profile in the UNIXPRIV class, and refresh the UNIXPRIV class. Then have the user reissue the command.

User Response: Contact your security administrator.

IRR52176I SHARED.IDS is defined, but application identity mapping is not implemented.

Explanation: You are attempting to assign a UID or GID in the OMVS segment, and the security administrator has indicated that shared UIDs and GIDs should be controlled. However, control of shared UIDs and GIDs requires the RACF database to be at least at stage 2 of application identity mapping, and this is not the case.

System Action: Command processing stops.

System Programmer Response: Use the IRRIRA00 utility to convert the RACF database to at least stage 2 of application identity mapping. See the RACF System Programmer's Guide for information about the IRRIRA00 utility. Once this is complete, the user may reissue the command.

RACF Security Administrator Response:

Either remove the SHARED.IDS profile from the

IRR52177I • IRR52181I

UNIXPRIV class, or contact the system programmer and have him implement application identity mapping.

User Response: Contact your security administrator or system programmer.

IRR52177I [User|Group] name was assigned an OMVS [UID|GID] value of id.

Explanation: In response to your request, a unique value, *id*, has been generated by RACF for the UID of user *name* or for the GID of group *name* in the OMVS segment. If a unique UID or GID value already existed in the OMVS segment of this USER or GROUP profile, then it is unchanged, and its value is what is displayed in this message. If a unique UID or GID value already existed, and RACF Remote Sharing Facility (RRSF) automatic command direction is in effect for the USER or GROUP class, then the command will be propagated with the OMVS UID or GID keyword specifying the preexisting value.

IRR52178I You cannot use automatic [UID|GID] assignment when a value already exists.

Explanation: You asked RACF to generate a unique value for either a UID or GID in the OMVS segment, however, a (non-unique) value already exists.

System Action: Command processing stops. The UID or GID is not changed.

User Response: If you want to use AUTOUID or AUTOGID to assign a new value, you must first delete the current value, and then reissue the command. A UID can be deleted using ALTUSER with the NOUID keyword. A GID can be deleted using ALTGROUP with the NOGID keyword. However, keep in mind that UNIX files may exist with the old UID or GID as the owner. You need to consider what to do with these files. For example, you might want to change file ownership such that the user or group continues to own them under the new UID or GID value. Given a user of BOB whose old UID was 50 and whose new UID is 100, this can be accomplished with the following UNIX command:

```
chown 100 $(find / -user 50)
```

This command can be used for groups as well by specifying "-group" instead of "-user". This command will not affect file systems which are currently unmounted. See the *z/OS UNIX System Services Command Reference* for details.

IRR52179I The BPX.NEXT.USER profile must be defined before you can use automatic [UID|GID] assignment.

Explanation: You asked RACF to generate a unique value for either a UID or GID in the OMVS segment, however, the BPX.NEXT.USER profile has not been defined in the FACILITY class.

System Action: Command processing stops.

RACF Security Administrator Response:

If you want users to be able to use the automatic UID/GID function, you must define the BPX.NEXT.USER profile with starting values for UIDs or GIDs in the profile's APPLDATA. See the *z/OS Security Server RACF Security Administrator's Guide* for details.

User Response: Contact your security administrator.

IRR52180I The BPX.NEXT.USER profile does not allow automatic [UID|GID] assignment.

Explanation: You asked RACF to generate a unique value for either a UID or GID in the OMVS segment, however, the BPX.NEXT.USER profile in the FACILITY class has not been set up to allow this.

System Action: Command processing stops.

RACF Security Administrator Response:

If you want users to be able to use the automatic UID/GID function, you must specify starting values (or ranges of values) for UIDs or GIDs in the profile's APPLDATA. See the *z/OS Security Server RACF Security Administrator's Guide* for details.

User Response: Contact your security administrator.

IRR52181I The BPX.NEXT.USER profile has run out of possible [UID|GID] values.

Explanation: In the course of automatically assigning UID or GID values, the maximum eligible value has been reached. RACF determines eligible UID and GID values by using the APPLDATA information of the BPX.NEXT.USER profile in the FACILITY class. If a single UID or GID value had been defined as a starting point, the maximum value of 2,147,483,647 has been reached. If a range of available UID or GID values had been defined, the upper bound of that range has been reached.

System Action: Command processing stops.

RACF Security Administrator Response:

Change the APPLDATA of the FACILITY class profile named BPX.NEXT.USER to specify an alternate starting point or range.

If RRSF is active, make sure the value you specify does not overlap with criteria specified in BPX.NEXT.USER on other RRSF nodes, or UID/GID collisions could occur across your network. If you are using automatic command propagation for the FACILITY class, make sure you use the ONLYAT keyword on the RALTER command when updating BPX.NEXT.USER or else your update will be propagated to the BPX.NEXT.USER profile on the other nodes.

User Response: Contact your security administrator.

IRR52182I Automatic [UID|GID] assignment requires application identity mapping to be implemented.

Explanation: The AUTOUID or AUTOGID keyword has been specified, but the RACF database has not been converted to the use of application identity mapping. Application identity mapping must be enabled in order for RACF to guarantee that the assigned UID or GID is unique. Use of the UNIXMAP class is not sufficient. The RACF database must be at least at stage 2 of application identity mapping.

System Action: Command processing stops.

System Programmer Response: Use the IRRIRA00 utility to convert the RACF database to at least stage 2 of application identity mapping. See the *z/OS Security Server RACF System Programmer's Guide* for information about the IRRIRA00 utility. Once this is complete, the user may reissue the command.

User Response: Contact your system programmer.

IRR52183I Use of automatic [UID|GID] assignment requires SHARED.IDS to be implemented.

Explanation: The AUTOUID or AUTOGID keyword has been specified, but shared UID/GID control has not been implemented. Shared UID/GID control must be implemented in order for RACF to guarantee that the assigned UID or GID is unique.

System Action: Command processing stops.

RACF Security Administrator Response:

You must implement the SHARED.IDS profile in the UNIXPRIV class in order to activate shared UID/GID control, which is a prerequisite for the automatic UID/GID function. See the *z/OS Security Server RACF Security Administrator's Guide* for details on shared UID/GID control. Once this is complete, the user may reissue the command.

User Response: Contact your security administrator.

IRR52184I You cannot use automatic [UID|GID] assignment with a list of names.

Explanation: You asked RACF to generate a unique value for either a UID or GID in the OMVS segment, but you specified a list of names on the command. Automatic id generation does not support this command syntax.

System Action: Command processing stops.

User Response: If you want RACF to assign a UID or GID value for each name, issue a separate command for each name.

IRR52185I The same [UID|GID] cannot be assigned to more than one [user|group].

Explanation: You tried to assign a UID to a list of users, or a GID to a list of groups, but shared UNIX ids are not allowed.

System Action: Command processing stops.

User Response: Issue a separate command with a different value for each name. If the names really require the same id, then reissue the command specifying the SHARED keyword. The SHARED keyword requires the SPECIAL attribute or READ authority to the SHARED.IDS resource in the UNIXPRIV class.

IRR52186I You cannot specify both [AUTOUID|AUTOGID] and SHARED.

Explanation: You specified either the AUTOUID or AUTOGID keyword and the SHARED keyword, but they are mutually exclusive.

System Action: Command processing stops.

User Response: Correct and reissue the command.

IRR52187I Incorrect APPLDATA syntax for the BPX.NEXT.USER profile.

Explanation: You have used the AUTOUID or AUTOGID keyword to request an automatically generated UID or GID. RACF derives the next available value using criteria specified in the APPLDATA field of the BPX.NEXT.USER profile in the FACILITY class. However, the APPLDATA contains a syntactically incorrect string.

System Action: Command processing stops.

RACF Security Administrator Response:

Correct the APPLDATA. The format of the APPLDATA is a valid UID value, or range of UID values, followed by a forward slash, followed by a valid GID value, or range of GID values. See the *z/OS Security Server RACF Security Administrator's Guide* for details on defining BPX.NEXT.USER.

If RRSF is active, make sure the value you specify does not overlap with criteria specified in BPX.NEXT.USER on other RRSF nodes, or UID/GID collisions could occur across your network. If you are using automatic command propagation for the FACILITY class, make sure you use the ONLYAT keyword on the RALTER command when updating BPX.NEXT.USER or else your update will be propagated to the BPX.NEXT.USER profile on the other nodes.

User Response: Contact your security administrator.

RACF cross-reference utility (IRRUT100) messages

IRR61000I Open failed for dd *ddn*

Explanation: The RACF cross-reference utility program was unable to open the data set specified by the specified ddname.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the data set resides.

IRR61001I Invalid input (80 character input record)

Explanation: A name supplied as input to the cross-reference utility program has more than 8 characters. The remaining records are scanned for errors.

System Action: The utility program stops.

IRR61002I Unauthorized user

Explanation: You are not defined to RACF or do not have sufficient authority to run the cross-reference utility program.

User Response: See your RACF security administrator.

IRR61003I Following names were not processed

Explanation: More than 1000 names were specified to the cross-reference utility program.

System Action: Those names over 1000 are listed and are not processed.

IRR61004I No occurrences of *name*

Explanation: The cross-reference utility program could not find the indicated name in the RACF database.

System Action: The utility program has ended successfully.

User Response: Check the name you entered and reissue the command.

IRR61006I SYSIN contains no valid input. Utility terminated

Explanation: The cross-reference utility program could not find valid input in SYSIN.

System Action: The utility program stops.

User Response: No input was found on SYSIN statement. You need to specify at least one name.

IRR61007I Insufficient authority to '*name*'; name ignored

Explanation: You are not authorized to list anything for the user ID or group name specified.

System Action: The name is ignored.

User Response: See your RACF security administrator.

RACF database verification (IRRUT200) messages

IRR62001I Unable to open DD *ddn* - processing terminated

Explanation: The verification utility program was not able to open the database with the specified ddname.

System Action: Processing stops.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the database resides.

internal work areas (buffers and work tables) in the IRRUT200 utility. The GETMAIN was unsuccessful. Probable cause: the storage was unavailable.

IRR62002I Unable to open DD SYSUT1 - copy function bypassed

Explanation: The verification utility program was not able to open the SYSUT1 data set.

System Action: The data set associated with DD SYSRACF has opened successfully and is used by the utility program.

Programmer Response: UT1 DD statement is used as the work data set in which IRRUT200 copies the database specified by SYSRACF DD statement for the copy function. If you want the RACF database to be used throughout processing, ignore this message. Otherwise, provide a usable work data set for SYSUT1 DD statement and rerun the utility.

IRR62007I Invalid control statement

Explanation: The verification utility program found that the control statement contains a delimiter or contents errors.

System Action: Processing stops.

Programmer Response: Verify that the SYSIN DD statement contains valid IRRUT200 control statements. For valid control statements, see *z/OS Security Server RACF System Programmer's Guide*.

IRR62003I Unable to open dd SYSRACF - SYSUT1 must contain RACF data set

Explanation: The verification utility program could not open the SYSRACF data set. The data set associated with DD SYSUT1 is assumed to contain a copy of the RACF database.

System Action: Processing continues.

Programmer Response: The database verification utility continues to process if it was unable to open the data set pointed to by SYSRACF DD statement. The utility assumes that the work data set (SYSUT1) contains a copy of the RACF database. Make sure that SYSRACF DD statement points to a RACF data set.

IRR62008I I/O ERROR - *jjj, sss, ddd, devtyp, ddn, oper, err, xxxx, acc*

Explanation: The verification utility program encountered a permanent I/O error while processing on device *ddd*. In the message text, the error analysis information provided by the SYNADAF data management macro instruction issued by the SYNAD routine was:

<i>jjj</i>	Job name
<i>sss</i>	Step name
<i>ddd</i>	Unit address of the device
<i>devtyp</i>	Device type
<i>ddn</i>	Data definition name
<i>oper</i>	Operation attempted
<i>err</i>	Error description
<i>xxxx</i>	Last seek address or block count
<i>acc</i>	Access method

This message can be caused by unformatted space at the end of the RACF database. Copying the RACF database with utilities other than IRRUT400 can cause unformatted space.

System Action: Utility processing stops.

User Response: Copy the database with IRRUT400 to format the space.

IRR62004I Insufficient storage - processing terminated

Explanation: A GETMAIN failed for the buffers and work areas necessary for the verification utility program to function. The request was for storage from subpool 0.

System Action: Processing stops.

Programmer Response: Get the message ID, any diagnostic information generated and contact your IBM support center.

Problem Determination: A GETMAIN was issued for

IRR62009I EOF on SYSIN - processing terminated

Explanation: The verification utility program found an unexpected end-of-file condition on the SYSIN data set.

System Action: Processing stops.

Programmer Response: Ensure that the END control statement is included in the SYSIN DD control statements to prevent an implied end of utility processing from occurring.

IRR62010I RACF data set not found - processing terminated

Explanation: A failure occurred when the verification utility program made a request to dynamic allocation for information retrieval.

System Action: Processing stops.

Programmer Response: Make sure SYSRACF DD statement specifies, as the data set name, the database you want to use during processing.

IRR62012I Insufficient storage for map function - request terminated

Explanation: A GETMAIN failed for the storage required by the verification utility program to perform the map function. The request was for storage from subpool 0.

System Action: Processing stops.

Programmer Response: This is an internal error. Get the message ID, any diagnostic information generated, and contact your IBM support center.

Problem Determination: A GETMAIN request was done for storage to process the BAM/allocation verification for the MAP function of the IRRUT200 utility. The GETMAIN failed. The probable cause is unavailable storage.

IRR62014I RBA of top level index block is invalid - may be an empty dataset - processing terminated

Explanation: The verification utility program found an error in the RBA (relative byte address) of the top level index block (in the ICB).

System Action: Processing stops.

Programmer Response: See “Problem Determination” for more detail. Use the BLKUPD command to correct the RBA of the top level index block. Also, make sure database is not empty.

Problem Determination: When this error occurs, the utility dumps the ICB in hexadecimal. Any one of the following conditions could cause this error in the ICB:

- The first 2 bytes are not zero.
- The last 4 bytes are zero.
- The last 12 bits are not zero (denoting an address not on a 4K boundary).

IRR62015I RBA of first BAM block is invalid - map function terminated

Explanation: The verification utility program found an error in the RBA (relative byte address) of the first BAM block (in the ICB).

System Action: Processing stops.

Programmer Response: See “Problem Determination” for more detail. Use the BLKUPD command to correct the RBA of first BAM block.

Problem Determination: When this error occurs, the utility dumps the ICB in hexadecimal. Any one of the following conditions could cause this error in the BAM:

- The last 4 bytes are zero.
- The first 2 bytes are not zero.
- The last 12 bits are not zero (denoting an address not on a 4K boundary).

IRR62017I Sequence set chain field is broken

Explanation: In processing all the index blocks, the verification utility program keeps a count of level 01 blocks. This count is used while processing the sequence set. While following the chain of level 01 blocks (sequence set), the utility program found a zero sequence set RBA (relative byte address) before the count of level 01 blocks was reached.

System Action: Utility processing stops.

Programmer Response: The current index block is dumped in hexadecimal. Use the BLKUPD command to correct the problem. Rerun the IRRUT200 utility.

IRR62018I Program limit exceeded - processing of index blocks terminated

Explanation: More than six levels of index blocks were found by the verification utility program.

System Action: Index block processing stops. after six levels have been processed. Level 01 blocks are not processed.

Programmer Response: Use the BLKUPD command to confirm that you have as many levels as reported by this message. If you do confirm this error, split the RACF database (using the range table) to correct the problem. For more information, see *z/OS Security Server RACF Diagnosis Guide*. If you cannot correct the problem, contact your IBM support center.

IRR62019I Unable to open DD SYSUT1 for READ after COPY function completed - processing terminated

Explanation: The RACF database verification utility program was not able to open the SYSUT1 data set for read after successfully copying the RACF database. The RACF database is defined by the SYSRACF DD statement.

System Action: Utility processing stops.

Programmer Response: Check for disk pack error messages related to SYSUT1 DD allocation; verify the characteristics of the data set for SYSUT1 and make sure they are correct. Rerun the IRRUT200 utility using the SYSUT1 data set for SYSRACF DD statement and

a work data set for SYSUT1. If the problem still occurs, run the IRRUT200 utility with the original database used prior to the error and do not use the copy function.

**IRR62021I Unable to load SYSUT1 -
unrecoverable I/O error on DD
SYSRACF - processing terminated**

Explanation: While reading the blocks from the RACF database defined by the SYSRACF DD statement, RACF encountered an unrecoverable error.

System Action: Utility processing stops.

Problem Determination: Message IRR62008I precedes this message and provides information about the I/O error.

IRR62022I Unable to load class descriptor table

Explanation: The verification utility program was not able to load the class descriptor table.

System Action: The verification utility program continues processing general classes using their class ID numbers instead of their class names.

IRR62023I Incorrect RACF dataset format

Explanation: One of the following problems occurred:

- The database name pointed to by the new format RACF database field (ICBDSFMT) of the inventory control block (ICB) for the SYSRACF DD statement is not a valid database.
- The inventory control block (ICB) does not have the correct information in the ICBID field.

System Action: Processing stops.

Programmer Response: Verify that your SYSRACF DD statement points to a database that was pre-formatted by RACF database initialization utility (IRRMIN00). Correct the problem and rerun the IRRUT200 utility.

Problem Determination: Make sure the database was initialized by the IRRMIN00 utility.

IRR62024I Segment table cannot be read

System Action: Processing stops.

Programmer Response: Verify that your SYSRACF DD statement points to a database that was pre-formatted by RACF database initialization utility (IRRMIN00). Correct the problem and rerun the IRRUT200 utility.

Problem Determination: An attempt was made by the RACF Database Verification utility to read the segment table associated with the templates for the data set specified by SYSRACF DD statement. The READ was unsuccessful because of one of the following:

- The database was not properly initialized by RACF Database Initialization utility (IRRMIN00).
- Reading of the database resulted in an end-of-file condition before the segment table was found.
- The segment table did not exist.

Ensure that the database is initialized and contains a set of templates and the associated segment table.

**IRR62025I Name of segment or profile in index
does not match equivalent in profile.
See the following.**

Explanation: The name and/or type of the profile do not agree between the index entry and the contents of the profile read. This message includes the following information about the error:

```
IRR62025I          Prof Type:  profile type
IRR62025I   Seg Name in Prof:  segment name in
                                the profile
IRR62025I   Seg Name in Index:  segment name in
                                the index
IRR62025I   Prof Name in Prof:  profile name in
                                the profile
IRR62025I   Prof Name in Index:  profile name in
                                the index
```

For example, in the following, the profile names do not match:

```
IRR62025I          Prof Type:  DATA SET
IRR62025I   Seg Name in Prof:  BASE
IRR62025I   Seg Name in Index:  BASE
IRR62025I   Prof Name in Prof:  PAYROLL.JULY.1987
IRR62025I   Prof Name in Index:  PAYROLL.JULY.1986
```

System Action: Processing continues.

Programmer Response: Use the BLKUPD command to correct the inconsistency.

Problem Determination: The error message indicates the index name and profile name in which the mismatch was found. Use this information to correct the inconsistency.

**IRR62026I BAM block chain field is broken - map
function terminated**

Explanation: While processing the chain of BAM blocks, IRRUT200 found a zero chain field in the BAM before all the blocks (the number contained in the ICB) were processed.

System Action: The map function stops.

Programmer Response: The BAM is dumped in hexadecimal when this error occurs. Use the BLKUPD command to correct the problem.

IRR62027I BAM block chain fields are in a loop - map function terminated

Explanation: IRRUT200 was processing the BAM when the count of the number of BAMs in the ICB was exceeded. The fields might be in a loop.

System Action: The map function stops.

Programmer Response: Use the BLKUPD command to confirm this error. If you do confirm this error, correct the problem using BLKUPD. For more information, see *z/OS Security Server RACF Diagnosis Guide*. If you cannot correct the problem, contact your IBM support center.

IRR62028I Count of BAM blocks in ICB is zero - map function terminated

Explanation: The ICB contains a count of zero for the number of BAM blocks in the RACF database.

System Action: The map function stops.

Programmer Response: Make sure your database was pre-formatted by the RACF Database Initialization Utility (IRRMN00). Also, ensure that SYSRACF DD statement points to the correct database you want to use.

IRR62029I Count of number of blocks defined by a BAM is invalid - map function terminated

Explanation: The count of the number of blocks defined by the BAM contained in the header is either zero or greater than 2038.

System Action: The map function stops.

Programmer Response: Make sure your database was pre-formatted by the RACF Database Initialization Utility (IRRMN00). Also, ensure that SYSRACF DD statement points to the database you want to use.

IRR62030I Data block failed validity check

Explanation: The data block pointed to by a level one index block does not begin with the value X'83'.

System Action: Processing stops.

Programmer Response: This is an internal error. The block in error is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic materials and contact your IBM support center.

IRR62031I Data block key length invalid

Explanation: The record name in the profile is not from 1 to 255 bytes in length.

System Action: Processing stops.

Programmer Response: This is an internal error. The

block in error is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic material and contact your IBM support center.

IRR62032I Displacement to free space is incorrect

Explanation: The offset (in the header of the index block) to the free space in the block is incorrect, or the end-of-block delimiter (X'0C') is not present.

System Action: Utility processing stops.

Programmer Response: This is an internal error. The particular index block is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic material and contact your IBM support center.

IRR62033I Displacement to last key is incorrect

Explanation: The offset (in the header of the index block) to the last entry is incorrect, or the entry identifier (X'21' or X'20') is not present.

System Action: Utility processing stops.

Programmer Response: This is an internal error. The index block is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic material and contact your IBM support center.

IRR62034I E(P) Byte/RBA of next block in sequence set is invalid

Explanation: The sequence set pointer entry in the level one index block is not preceded by the value X'6x', or the next level one block is not valid for one of the following reasons:

- The first 2 bytes are not zero.
- The last 4 bytes are zero and this is not the last block in the chain.
- The RBA is not a multiple of 4096.

System Action: Utility processing stops.

Programmer Response: The index block is dumped in hexadecimal. Use the BLKUPD command to correct the problem in the index. Rerun the IRRUT200 utility.

IRR62035I E(P) Byte/RBA xxxxxxxxxxxx Failed validity check

Explanation: The pointer entry of an index entry in the block is not preceded by the value X'6x', or the RBA xxxxxxxxxxxx of the next level index block or profile is not valid for one of the following reasons:

- The first 2 bytes are not zero.
- The last 4 bytes are zero.
- The RBA is not a multiple of 4096.
- For level one blocks, the RBA is not a multiple of 256.

IRRUT200 does not dump the index block if only the RBA is not valid.

System Action: Utility processing stops.

Programmer Response: If the RBA was not valid, no dump is produced. Otherwise, a hexadecimal dump is produced. Use the BLKUPD command to correct the problem.

IRR62036I End of data flag byte possibly missing

Explanation: The end-of-block delimiter at the end of the index block is not X'0C' or the displacement to this byte is incorrect. The displacement is calculated by adding the sum of the length of the last entry name in the block and the length of the pointer entry to the offset of the last entry name in the block. If the length of the entry name is incorrect, the displacement to this byte is incorrect.

System Action: Utility processing stops.

Programmer Response: The block in error is dumped in hexadecimal. Use the BLKUPD command to correct the problem. Rerun the IRRUT200 utility.

IRR62037I Following Level 01 block is not pointed to by a Level 02 block

Explanation: An index block with a level greater than X'02' points to an index block with a level of X'01' in the header. IRRUT200 processes the level one index block normally.

System Action: Processing continues.

Programmer Response: The level one index block was processed. You may want to run the IRRUT200 utility against your database again to check for any remaining errors.

IRR62038I I/O error rereading BAM block - map function terminated

Explanation: IRRUT200 encountered an unrecoverable I/O error while attempting to reread a BAM block. The block is not dumped.

System Action: MAP function stops.

Programmer Response: An I/O error message was generated prior to this message (IRR62008I). Use this message to determine the cause of the I/O error.

IRR62039I Index block failed validity check

Explanation: The block does not begin with the value X'8A'.

System Action: Utility processing stops.

Programmer Response: Use the BLKUPD command to confirm this error. If you confirm this error, correct the problem using BLKUPD. For more information, see

z/OS Security Server RACF Diagnosis Guide. If you cannot correct the problem, contact your IBM support center.

IRR62040I Invalid E(K) byte in key entry at offset

Explanation: An index entry name might not be preceded by a valid key byte. All entries in index blocks that are not level one must begin with the value X'21'. In level one index blocks, either X'22' or X'21' must precede each entry except for the last entry, which must be preceded by X'20'.

System Action: Processing continues.

Programmer Response: Use the BLKUPD command to correct the problem.

IRR62041I Key entry length invalid at offset *offset*

Explanation: An index entry name does not have a valid length. An entry other than the first entry in a block that is not level one, might have a zero length. If it does, it must also have a compression count other than zero. The compression count must not be greater than the length of the first entry in the block. The offset indicated in the message is the offset of the beginning of the incorrect entry in the index block.

System Action: Utility processing stops.

Programmer Response: Use the BLKUPD command to confirm this error. If you do confirm this error, correct the problem using BLKUPD. For more information, see *z/OS Security Server RACF Diagnosis Guide*. If you cannot correct the problem, contact your IBM support center.

IRR62042I Logical length of data block is invalid

Explanation: The logical length of the profile is not a multiple of 256 or is greater than the allocated length as defined in the header.

System Action: Utility processing stops.

Programmer Response: Use the BLKUPD command to confirm this error. If you do confirm this error, correct the problem using BLKUPD. For more information, see *z/OS Security Server RACF Diagnosis Guide*. If you cannot correct the problem, contact your IBM support center.

IRR62043I More than 200 BAM allocation errors found

Explanation: In verifying the BAM blocks with the actual allocation of segments in the RACF database, IRRUT200 found more than 200 locations with possible conflicts.

System Action: Utility processing stops.

Programmer Response: Make sure you are

IRR62044I • IRR62055I

processing with the correct database. Also, ensure that you have a database at the right release level and properly initialized.

IRR62044I Non Level 01 index block is in sequence set

Explanation: The index block is in the sequence set, but the level in the header is not one.

System Action: Processing stops.

Programmer Response: The block in error is dumped in hexadecimal. Use the BLKUPD command to correct the problem.

IRR62045I Possible compression count error in key entry at offset *offset*

Explanation: An index entry name might not have a valid compression count. The first entry must have a zero compression count. An entry, other than the first entry, must have a compression count which is less than or equal to the length of the first entry name. The offset indicated in the message is the offset of the beginning of the incorrect entry in the index block.

System Action: Processing continues.

Programmer Response: At the completion of the utility processing, you can use the offset from the message and correct the problem by using BLKUPD command.

IRR62046I Possible loop in sequence set

Explanation: The first entry name of the level one index block is not alphabetically greater than the first entry name of the previous level one index block.

System Action: Utility processing stops.

Programmer Response: Use the BLKUPD command to confirm this error. If you do confirm this error, correct the problem using BLKUPD. Note that if both blocks contain X'22', they are valid duplicates. For more information, see *z/OS Security Server RACF Diagnosis Guide*. If you cannot correct the problem, contact your IBM support center.

IRR62048I RBA invalid for template at offset *offset* RBA *rba*

Explanation: In the ICB, the indicated RBA for the template at the indicated offset is not valid. The RBA is not valid for one of the following reasons:

- The first 2 bytes are not zero.
- The last 4 bytes are zero.
- The RBA is not a multiple of 4096.

System Action: Processing continues.

Programmer Response: A dump is provided in

hexadecimal. Use the BLKUPD command to correct the problem.

IRR62050I RBA of first block of index sequence set is invalid

Explanation: The RBA of the first block of the index sequence set (in the ICB) is not valid for one of the following reasons:

- The first 2 bytes are not zero.
- The last 4 bytes are zero.
- The RBA is not a multiple of 4096.

System Action: Processing stops.

Programmer Response: A dump is provided for the block in error. Use the BLKUPD command to correct the problem.

IRR62051I RBA of next BAM block is invalid - map function terminated

Explanation: The RBA of the next BAM block is not valid for one of the following reasons:

- The first 2 bytes are not zero.
- The RBA is not a multiple of 4096.

System Action: Map function stops. A hexadecimal dump is provided.

Programmer Response: Using the information from the explanation and the dump, use the BLKUPD command to correct the problem.

IRR62053I Read failed for top level index block - processing terminated

Explanation: A permanent I/O error occurred while attempting to read the top-level index block. The block is not dumped.

System Action: Processing stops.

Programmer Response: Message IRR62008I contains the specifics regarding the I/O error. Use this information to determine the cause of the problem.

IRR62055I Template count in ICB is invalid

Explanation: The ICB contains a count of the number of templates that is either zero or greater than the number of spaces allocated for template definitions.

System Action: Processing stops.

Programmer Response: Make sure that your database has been properly initialized by RACF Database Initialization Utility (IRRMIN00). Also, make sure the SYSRACF DD statement points to the correct database.

IRR62056I Top level index block failed validity check - processing terminated

Explanation: The top-level index block, pointed to by the ICB, does not begin with the value X'8A'.

System Action: Processing stops.

Programmer Response: Make sure your database has been properly initialized by the RACF Database Initialization Utility (IRRMN00). Also, make sure that SYSRACF DD statement points to the correct database.

IRR62057I Unrecoverable logic error detected during name verification

Explanation: An error occurred within the utility.

System Action: Processing stops.

Programmer Response: Report this problem to your IBM support center.

IRR62058I The offset table pointer for the above index block failed a validity check

Explanation: This message is issued as part of the validity checking done by this utility.

Programmer Response: Use the BLKUPD command to investigate and correct the error.

IRR62059I The offset table entry count for the above index block failed a validity check

Explanation: This message is issued as part of the validity checking done by this utility.

Programmer Response: Use the BLKUPD command to investigate and correct the error.

IRR62060I The count of names in the above index block statistics does not equal the offset table count of *count*

Explanation: This message is issued as part of the validity checking done by this utility.

Programmer Response: Use the BLKUPD utility to investigate and correct the error.

IRR62061I The offset table pointer at index position *position* has failed a validity check for the above index block

Explanation: This message is issued as part of the validity checking done by this utility.

Programmer Response: Use the BLKUPD command to investigate and correct the error.

IRR62062I The offset table pointer at index position *position* does not point to a valid entry in the above index block

Programmer Response: Use the BLKUPD command to investigate and correct the error.

IRR62063I Zero segment count found during [MAP | INDEX] processing for entry at offset *offset*.

Explanation: A segment count of zero was detected in an index entry beginning at offset *offset*. This is an incorrect state in that all index entries should have one or more segments.

System Action: Utility processing continues. A return code of 8 is issued. BAM allocation errors (BAM=ALLOC ACTUAL=UNALLOC) are flagged during MAP processing for valid entries in the block containing the failing entry.

For index processing, statistics are not compiled for the failing index block. Validation continues with the next index entry.

Map processing stops for the failing block. It continues with the next block.

Programmer Response: A dump is provided for the index block in error if INDEX was requested. The offset of the index entry containing the incorrect segment count is included in this message text. (If only MAP processing was requested, running IRRUT200 another time requesting INDEX FORMAT can help identify the block in which the error occurred.) Determine whether it is easier to delete or correct this entry. In either case, refer to the *z/OS Security Server RACF Diagnosis Guide* for index entry formats.

If it is decided that the entry should be deleted, do so using the BLKUPD command. After deletion, MAP processing shows BAM allocation errors (BAM=ALLOC ACTUAL=UNALLOC) for the BAM associated with the deleted profile. These errors can be resolved using the RACF database utility (IRRUT400).

If it is decided that the entry should be corrected, do so using BLKUPD.

Upon completion of index entry correction or deletion, IRRUT200 must be run against the updated database to ensure complete validation. IRRUT200 bypasses validation for index entries containing a zero segment count. Data block verification is bypassed during map processing for all entries in the data block following the entry in error.

IRR62064I Serialization is not held while verifying the database associated with DD SYSUT1

Explanation: This is an informational message. It appears at the end of the DD SYSUT2 data set only

IRR62065I • IRR63002I

when the SYSUT1 DD statement is specified and the SYSRACF DD statement is absent from your JCL.

Programmer Response:

- If the IRRUT200 utility ran without errors, the message is informational only; no response is needed.
- If the DD SYSUT1 data set has specified the active database, and database updates were performed while the IRRUT200 utility was running, database errors may have been reported. Database errors reported in this instance are not necessarily true database errors. Either rerun the job without making database updates while the job is running, or specify a DD SYSRACF statement to take advantage of the serialization on the data set.

IRR62065I IEBGENER copied SYSRACF to the work data set SYSUT1, IEBGENER RC=return_code

Explanation: When a SYSUT1 DD statement is specified, IRRUT200 links to the MVS utility IEBGENER. IEBGENER copies the database pointed to by the SYSRACF DD statement to a work data set pointed to by the SYSUT1 DD statement. A return code of 0 or 4 indicates that IEBGENER successfully copied the database. However, a return code of 4 indicates some mismatch in the output and input data set attributes.

System Action: With the work data set copied, the verification of the database continues.

User Response: For a return code of 4, correct the data set pointed to by the SYSUT1 DD statement so that it has the same attributes as the database pointed to by the SYSRACF DD statement.

IRR62066I IEBGENER failed to copy SYSRACF to the work data set SYSUT1, IEBGENER RC=return_code

Explanation: When a SYSUT1 DD statement is specified, IRRUT200 links to the MVS utility IEBGENER. IEBGENER copies the database pointed to by the SYSRACF DD statement to a work data set pointed to by the SYSUT1 DD statement. IEBGENER

could not copy the database and IRRUT200 ends processing.

System Action: IRRUT200 ends processing.

User Response: Refer to the appropriate MVS documentation for an explanation of the IEBGENER return codes. Correct the problem and resubmit the job.

IRR62067I Database copy (SYSRACF to SYSUT1) failed due to incompatible device types.

Explanation: The database (SYSRACF) and work data set (SYSUT1) have incompatible device types.

System Action: Processing ends with a return code of 12.

Programmer Response: Do one of the following:

- Use the RACF Database Split/Merge/Extend utility program (IRRUT400) to copy a database to or from devices with different track geometries.
- Create a work data set (SYSUT1) on a device that is compatible with the database you are copying (SYSRACF).

Run the IRRUT200 utility again.

IRR62068I Base profile structure of alias entry contains an error.

Explanation: An error was found in the base profile structure of an alias index entry. The structure should contain the number of base profiles that correspond to this alias name, followed by the length and name of each base profile. The count of base profiles might not match the actual number of entries in the structure, or the length of an entry might be incorrect.

System Action: The block containing the error is printed, and utility processing continues with the next block.

Programmer Response: Use the BLKUPD command to confirm and correct the problem. For more information, see the *z/OS Security Server RACF Diagnosis Guide*.

RACF Block Update Command (BLKUPD) messages

IRR63001I Invalid command.

Explanation: One of the following situations occurred:

- The command is unknown.
- The command is a subcommand of READ and was entered without first entering the READ command.
- The command is a subcommand of READ or DISPLAY that attempts to update the RACF database, but UPDATE was not specified on the READ command.

- A READ (or DISPLAY) is in progress but the command entered is not a subcommand of READ (or DISPLAY).

System Action: The command is ignored.

Programmer Response: Enter another command.

IRR63002I Offset is offset

Explanation: The search argument specified on the FIND command was located at the hexadecimal value

xxx in the specified NEW or OLD block.

Programmer Response: Enter another command if desired.

IRR63003I String not found.

Explanation: The search argument in the FIND command was not located in the specified NEW or OLD block.

Programmer Response: Enter another command.

Problem Determination: To view the contents of the NEW or OLD block, use the LIST or FORMAT command.

IRR63004I REPLACE complete.

Explanation: The operation requested by the REP command is completed.

Programmer Response: Enter another command.

IRR63005I VERIFY failed. REPLACE not done.

Explanation: The string specified in the VER keyword of the REP subcommand was not found at the given offset, or the string extended beyond the end of the block.

System Action: The string was not replaced. The command is ignored.

Programmer Response: Enter another command.

Problem Determination: To view the contents of the NEW block, use the LIST or FORMAT command.

IRR63006I READ ended. Block not saved.

Explanation: The function initiated by the READ command is ended and nothing is saved in response to the END command.

System Action: The block was not written back to the RACF database because either NOSAVE was specified, or no changes were made to the block, or UPDATE was not specified on the READ command.

Programmer Response: Enter a READ, LOCATE, or END command.

IRR63007I UPDATE causes block overflow. NO changes made.

Explanation: The REP, or CHANGE and INSERT (under DISPLAY) operation is ignored because the modified block would be greater than 4096 bytes.

System Action: The command is ignored.

Programmer Response: Enter another command.

Problem Determination: To view the contents of the NEW block, use the LIST or FORMAT command.

IRR63008I Old block recopied into new block.

Explanation: The REREAD subcommand of READ is complete. The NEW block is the same as the OLD block.

Programmer Response: Enter another command.

IRR63009I DISPLAY ended. Changes saved.

Explanation: The DISPLAY function is ended and the updates saved. The block may be changed further by subcommands of READ. The END SAVE subcommand of READ updates the RACF database with this block.

Programmer Response: Enter another command.

IRR63010I DISPLAY ended. Changes not saved.

Explanation: The DISPLAY function has ended without saving the changes made in response to the END (with NOSAVE) command, or because UPDATE was not specified on the READ command.

Programmer Response: Enter a subcommand of READ.

IRR63011I Invalid data in index block. DISPLAY ended.

Explanation: The entry identifier or the length in the index is not correct.

System Action: The DISPLAY function is ended and any changes made are not saved.

Programmer Response: To correct the entry, use the LIST and REP subcommands of READ. Enter the DISPLAY subcommand again.

Problem Determination: Record message number and RBA of READ command. Get a dump of the area you are trying to DISPLAY and check the data of the entry which had the error. Contact your IBM support center.

IRR63012I Block is not a valid index block.

Explanation: The block that is the object of a FORMAT or DISPLAY command is not a valid index block. The following tests are made for a valid index block:

- The first index block identifier (offset 00) must be X'8A'.
- The second index block identifier (offset 03) must be X'4E'.
- The displacement to free space must be greater than the displacement to the last entry.
- The displacement to free space must be less than 4096.
- The last byte before free space (the end of block delimiter) must be X'0C'.

IRR63013I • IRR63018I

- The entry identifier for all entries must be X'21' or X'22', except for the identifier of the last entry in a level 01 block, which must be X'20'.
- The lengths of all entries must be correct.
- The pointer section identifier—also called the E(P) byte—of each entry must be X'62' or X'66'.

System Action: The command is ignored.

Programmer Response: Make sure the RBA specified on the READ command is that of an index block. Use the LIST and REP subcommands of READ to fix the index block.

Problem Determination: Record message number and RBA of READ command. Get a dump of the area you are trying to DISPLAY or FORMAT and check the data of the index which had the error. Contact your IBM support center.

IRR63013I READ ended. Block saved.

Explanation: The function initiated by the READ command is ended.

System Action: The modified block is saved in the RACF database.

Programmer Response: Enter a READ, LOCATE, or END command.

IRR63014I Record not found.

Explanation: The RBA (relative byte address) specified on a READ command is not within the extents of the RACF database.

System Action: The command is ignored.

Programmer Response: Enter another READ command for a block within the RACF database.

IRR63015I Open failed for DD SYSRACF.

Explanation: The BLKUPD command could not open the RACF database defined by the SYSRACF DD statement.

System Action: The BLKUPD command is ended.

Programmer Response: Allocate the RACF database to DD SYSRACF and retry.

Problem Determination: Find out if the DD SYSRACF is already allocated to a data set.

IRR63016I I/O error - *jjj*, *sss*, *ddd*, *devtyp*, *ddn*, *oper*, *err*, *xxxx*, *acc*

Explanation: The BLKUPD command encountered a permanent I/O error while processing on device *ddd*.

System Action: Command processing ends with a return code 12.

Programmer Response: Examine the text of the

message displayed on the terminal and match the error with codes in "Problem Determination."

Problem Determination: In the message text, the error analysis information provided by the SYNADAF data management macro instruction issued by the SYNAD routine was:

<i>jjj</i>	Job name
<i>sss</i>	Step name
<i>ddd</i>	Unit address of the device
<i>devtyp</i>	Device type
<i>ddn</i>	Data definition name
<i>oper</i>	Operation attempted
<i>err</i>	Error description
<i>xxxx</i>	Last seek address or block count
<i>acc</i>	Access method

IRR63017I Entry not found. Logical level 1 follows.

Explanation: The entry specified in a LOCATE command cannot be found. The level 1 block that ought to contain the specified entry is displayed.

Programmer Response: Enter a READ, LOCATE or END command. To add the entry to the block, use the DISPLAY subcommand of READ.

Problem Determination: To view the contents of the index block, use the LIST or FORMAT command.

IRR63018I Index block chain for entry is broken.

Explanation: A block in the chain for a LOCATE command search is not a valid index block. The following tests are made for a valid index block:

- The same tests are made as shown for message IRR63012I.
- The RBA (relative byte address) for the next byte on the chain must be nonzero, with the two high order bytes zero, and represent an address on a 4K boundary within the extent of the RACF database.
- The level of the block must be below the level of the previous block on the chain.

System Action: The block is dumped in hexadecimal.

Programmer Response: Correct the block in error by using the READ command and its subcommands.

Problem Determination: Run the IRRUT200 utility against the RACF database to find the troubled area.

IRR63019I Error in sequence set. Index block at RBA *rba*.

Explanation: The sequence set block at the specified RBA (relative byte address) contains an error. The following tests are made for a valid block:

- The block must be in collating sequence with the previous block on the sequence set.
- The first index block identifier (offset 00) must be X'8A'.
- The second index block identifier (offset 03) must be X'4E'.
- The displacement to free space must be greater than the displacement to the last entry.
- The displacement to free space must be less than 4096.
- The last byte before free space (the end of block delimiter) must be X'0C'.
- The entry identifier of the last entry in the block must be X'20'.
- The entry identifier for all other entries must be X'21' or X'22'.
- All entries must have correct lengths and pointer section identifiers of X'62' or X'66'.
- The block must be a level 01 block.
- The RBA (relative byte address) for the next byte in the sequence set must be nonzero, with the two high-order bytes zero, represent an address on a 4K boundary within the extent of the RACF database, and be not more than 4 bytes long.

System Action: The block is dumped in hexadecimal.

Programmer Response: Correct the block in error by using the READ command and its subcommands.

Problem Determination: Examine the hexadecimal dump of the index block. Run the IRRUT200 utility against the RACF database to find the index problem.

IRR63020I Entry not found. DISPLAY ended.

Explanation: The DISPLAY command specified an entry that could not be found in the index block.

System Action: The command is ignored.

Programmer Response: Reenter the DISPLAY command with an existing entry.

IRR63021I BLKUPD ended due to error+ Unable to establish ESTAE.

Explanation: The BLKUPD command ended due to a system error. An ESTAE recovery environment could not be established.

System Action: Command processing ends with a return code of 12.

Programmer Response: Enter the BLKUPD

command again. If the problem persists, ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

Problem Determination: Examine system abend code and return code to determine the cause of the ESTAE setup failure.

IRR63022I Command not processed due to error+ *routine-name* return code is *return-code*

Explanation: The TSO/E service routine indicated in the message failed with a return code of *xx*.

System Action: Command processing ends with a return code of 12.

Programmer Response: Refer to the documentation containing the service routine for an explanation.

Problem Determination: For an explanation of the TSO/E service routines return codes, see *z/OS TSO/E Programming Services*. For the order number of the document you need, see *z/OS TSO/E General Information*.

IRR63023I Key length error+ Compression count plus key length must be from 1 to 255 characters.

Explanation: After processing a CHANGE or INSERT command, the compression count plus the key length of the new entry is less than 1 or greater than 255.

System Action: The command is ignored.

Programmer Response: Adjust the length or compression count so that the sum is 255 or less. Enter the command again.

Problem Determination: To view the contents of the index block, use the LIST or FORMAT command.

IRR63024I Invalid ICB. LOCATE ended.

Explanation: The LOCATE command found the ICB in the RACF database contains incorrect data. The sequence set RBA or the RBA of the first index block in the ICB is zero or not on a 4K boundary.

System Action: The LOCATE command is ignored.

Programmer Response: Correct the ICB using the READ command and its subcommands. Check that the database used is the correct RACF database.

Problem Determination: Run the IRRUT200 utility against the RACF database to find the error.

IRR63025I • IRR63039I

IRR63025I Entry found.

Explanation: The entry requested by the LOCATE command was found with a sequence set search.

System Action: The index block containing the entry is displayed.

Programmer Response: Enter another command.

IRR63032I Segment not defined in templates.

Explanation: The segment name specified does not match any of the segments defined in the templates.

System Action: Command fails.

Programmer Response: Check the segment name that was specified as the SEGMENT parameter.

IRR63033I Base segment cannot be specified.

Explanation: The segment name of BASE specified on the command is incorrect. Only the RBA of the BASE segment can be updated.

System Action: Command fails.

Programmer Response: Check the segment name that was specified as the SEGMENT parameter.

IRR63034I Segment already exists.

Explanation: The segment name specified on the INSERT command already is defined to the current entry.

System Action: Command fails.

Programmer Response: Check the segment name that was specified as the SEGMENT parameter.

IRR63035I Storage allocation failed.

Explanation: The GETMAIN of storage for this module failed.

System Action: Processing ends with a return code of 12.

Programmer Response: Try the command again. If the same error occurs, check for a problem with storage management. Should storage management be fine, record this error and call your IBM support center.

Problem Determination: Examine the abend and return code from GETMAIN. Refer to the proper documentation for details about failure codes.

IRR63036I The first index entry has been deleted. The rest of the index block may need to be updated.

Explanation: The programmer just deleted the first index entry of an index block.

Programmer Response: Check the rest of the index entries for front-end compression. If they were compressed they might need to be decompressed to avoid errors in the index block.

Problem Determination: Use the FORMAT command to view the NEW block to analyze the index block which has been updated.

IRR63037I The first index entry has been changed. The rest of the index block may need to be updated.

Explanation: The programmer just changed the first index entry of an index block.

Programmer Response: Check the rest of the index entries for front-end compression. If they were compressed they might need to be decompressed to avoid errors in the index block. Also check that the index entries are still in collating sequence.

Problem Determination: Use the FORMAT command to view the NEW block to analyze the index block which has been updated.

IRR63038I The first index entry has been inserted. The rest of the index block may need to be updated.

Explanation: The programmer just inserted a new first index entry into the current index block.

Programmer Response: Check the rest of the index entries for front-end compression. If they were compressed they might need to be decompressed to avoid errors in the index block. Also check that the index entries are still in collating sequence.

Problem Determination: Use the FORMAT command to view the NEW block to analyze the index block which has been updated.

IRR63039I Segment does not exist.

Explanation: The segment name specified on the SEGMENT keyword of the CHANGE or DELETE commands is not defined to the current index entry.

System Action: Command fails.

Programmer Response: DISPLAY the index entry again and examine it to be sure it is the correct entry. If the segment you wish to update is not there, use the INSERT command to insert it.

Problem Determination: Use the DISPLAY command to view the index entry and its segments.

IRR63040I Input data set is invalid. Processing terminated.

Explanation: The data set specified on the BLKUPD command is not a valid format RACF data set.

System Action: The BLKUPD command ends with a return code of 12.

Programmer Response: Check the data set name. Be sure the data set block size is 4096. Call your IBM support center with this message number and a listing of the data set you are trying to use with BLKUPD.

IRR63041I Could not read the ICB.

Explanation: The RACF data set specified on the BLKUPD command could not be validated for its format because the ICB could not be read.

System Action: BLKUPD command processing ends with a return code of 12.

Programmer Response: Check the data set name. Be sure the data set block size is 4096.

Problem Determination: Run the IRRUT200 utility to validate the RACF data set and to point out any discrepancies. Call your IBM support center with this message number and a listing of the data set you are trying to work with.

IRR63042I This is not a level 1 index block, no segment information is available.

Explanation: The index block that was read in by the READ command is not a level-1 index block. The SEGMENT keyword of the DISPLAY command and its subcommands is only valid for level-1 index blocks.

System Action: The subcommand of DISPLAY (CHANGE, INSERT, or DELETE) fails, and utility processing continues.

System Programmer Response: End processing of the DISPLAY command and perform a FORMAT subcommand under READ. Determine the level of the index block being listed by the output of the FORMAT subcommand. Reassess which level-1 index block RBA you intended to work with, END the READ command, and issue the READ command with the RBA of the level-1 index block.

IRR63043I The ICB indicates the input data set is not a Restructured Database. The ICB may be corrupt. Processing Continues.

Explanation: The ICBDSFMT field of the ICB, for the RACF database specified on the BLKUPD command, indicates that the database supplied is not a restructured RACF database.

System Action: Utility processing continues.

System Programmer Response: Use the BLKUPD/READ/LIST ALL command to examine the ICB and assess the extent of the damage to the ICB. If the ICB is extensively damaged, call your IBM support center with this message number and a listing of the data set you are trying to update.

IRR63044I BLKUPD UPDATE processing is not permitted while the system is in read-only mode.

Explanation: A BLKUPD command was entered requesting UPDATE of the RACF data set. The system is currently in read-only mode and updating of the RACF data set is not allowed.

System Action: The BLKUPD command is not processed.

System Programmer Response: To make a change to the RACF data set, you can do one of the following:

- Issue BLKUPD from another system that is not in read-only mode.
- Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and reissue the BLKUPD READ UPDATE.
- Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode and reissue the BLKUPD READ UPDATE.

IRR63045I A coupling facility related error has occurred. BLKUPD processing has ended abnormally.

Explanation: An error occurred when accessing the coupling facility.

System Action: BLKUPD processing ends abnormally.

System Programmer Response: Check the information specified in IRRX016I, which is issued to the system console. Changes requested via BLKUPD may or may not have taken effect. Verify these changes after the coupling facility related error has been corrected. Reissue BLKUPD again, as necessary.

IRR63046I The BLKUPD command does not support the keyword *keyword*.

Explanation: An undefined keyword was encountered during processing of the BLKUPD command.

System Action: The command is not processed.

User Response: Check the command syntax and issue the command again.

Operator Response: None.

RACF database split/merge utility (IRRUT400) messages

IRR65000I • IRR65009I

IRR65000I Invalid input to message writing routine attempting to write message number *message-number*.

Explanation: This is an error internal to the utility. The specified *message-number* was not found.

System Action: System processing continues.

Problem Determination: Record the specified message number and contact your IBM support center.

IRR65001I Element number *number* of range table is out of sequence.

Explanation: The indicated range table entry is out of collating sequence.

System Action: Utility processing stops.

System Programmer Response: Ensure that the range table was assembled and link-edited correctly. Correct the order of the entries which are out of sequence. For information on using a range table, see *z/OS Security Server RACF System Programmer's Guide*.

Problem Determination: Verify that each entry in the range table appears with its keys in ascending order.

IRR65002I Unable to load module *table-name* to be used as range table.

Explanation: The load module named in the TABLE keyword could not be loaded into storage.

System Action: Utility processing stops.

System Programmer Response: A STEPLIB DD statement might be missing.

IRR65003I *error-type* on *ddname* attempting a request of block at RBA *rba*.

Explanation: The indicated error occurred while attempting a BDAM read (READ), BDAM write (WRITE), or BSAM write (LOAD).

System Action: The *ddname* of the file on which the error occurred is listed, along with the RBA (relative byte address) of the byte being accessed.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the database resides.

IRR65004I Range table contains no elements or first element string is not binary zeros.

Explanation: The first fullword of the range table is binary zeros, indicating no elements in the table, or the string portion of the first element is not binary zeros, as is required.

System Action: Utility processing stops.

Programmer Response: Ensure that the range table was assembled and link-edited correctly. For information on using a range table, see *z/OS Security Server RACF System Programmer's Guide*.

IRR65005I RACF data set full on *ddname*.

Explanation: Space has been exhausted on the specified output RACF database.

System Action: Utility processing stops.

System Programmer Response: Increase the size of the output database.

Problem Determination: This message is accompanied by message number IRR65018I, which can be used to determine how much data has already been processed.

IRR65006I Unable to open *dsname*, *ddname*.

Explanation: If the database is for input, the utility stops processing. If the database is for output, only processing to that database ends.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the database resides.

IRR65007I Information retrieval for *ddname* failed with error code *code*.

Explanation: RACF issued a dynamic allocation request (SVC 99) for information about the *ddname* indicated in the message. However, the return code from dynamic allocation was unexpected.

System Programmer Response: See "Problem Determination."

Problem Determination: Check the return code from the SVC 99 in *z/OS MVS Programming: Authorized Assembler Services Guide*.

IRR65008I *dsname* successfully opened for *open-type* on *ddname*.

Explanation: The named database has been successfully opened (BSAM open for INITIALIZATION or BDAM open for PROCESSING) with the given *ddname*.

System Action: Utility processing continues normally.

IRR65009I No input DD statements found - Processing terminated.

Explanation: The utility cannot perform without at least one input RACF database.

System Programmer Response: Ensure that at least one DD statement has been allocated.

Problem Determination: Check the JCL DD statements to verify this.

IRR65010I LOCK function requested, *ddname* already / now locked.

Explanation: To prevent updates to the database indicated by *ddname*, the LOCK function is requested. If the database was not located previously, it is locked at this time.

System Action: Utility processing continues.

IRR65011I Lock recovery *disposition* successful for *ddname*.

Explanation: This message reports the results of the attempt to turn the extend bit OFF in the ICB for the listed *ddname*. If lock recovery is not successful, the bit remains ON in that ICB. If lock recovery is successful, the bit has been turned OFF.

System Action: Utility processing continues.

IRR65012I *profile-name* in class *class-name* from *ddname* is duplicate of same name from *ddname*.

Explanation: The named profile could not be copied to an output database because it has the same name as a profile already copied from another input database. Either the profile is in a class other than DATASET or the NODUPDATASETS option is in effect.

System Action: Utility processing stops.

Problem Determination: Check the PARM field of the EXEC statement for this utility. For duplicate names, option DUPDATASETS must be in effect. Also, check to see what class the profile is actually in.

IRR65013I Index entry *entry-name* on *ddname* points to a tape volume set of which it is not a member.

Explanation: The index entry indicated by *entry-name* does not appear in the volume list of the profile for the tape volume set to which it points.

System Action: The index entry is not copied to an output database. The tape volume set is copied if no other errors exist.

System Programmer Response: See "Problem Determination."

Problem Determination: Ensure that the index entry and database specified by DD statement are both correct.

IRR65014I A tape volume set from *ddname* is inconsistent with the range table, member names follow: *member-name member-name ...*

Explanation: The range table specified with the TABLE keyword does not designate all of the members of the set to be copied to the same output database. The member names listed are not prefixed by the characters TAPEVOL-, but the prefix was used when interrogating the range table.

System Action: The tape volume set is not copied to output.

IRR65015I A tape volume set from *ddname1* contains a duplicate of *entry-name* from *ddname2*, member names follow: *member-name member-name ...*

Explanation: Two tape volume sets contain the same name in their volume lists. Therefore, only one of the sets can be copied to the output database.

System Action: The entire tape volume set whose members are listed is not copied to output.

IRR65016I *abend-code* abend during utility processing.

Explanation: The specified abnormal termination occurred during the execution of the utility.

System Action: Utility processing stops.

System Programmer Response: See "Problem Determination."

Problem Determination: Use the indicated abend code and any previous messages issued by this utility, to determine the appropriate action. See your MVS system codes documentation for more information about the abend indicated in the message.

IRR65017I Unable to establish recovery environment. Processing terminated.

Explanation: Processing stops because adequate recovery cannot be provided.

System Action: Utility processing stops.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, contact your IBM support center.

IRR65018I Output processing to *ddname* terminated while processing entry *entry-name*.

Explanation: Because of an error identified by the message immediately preceding this message on the output, no further processing of the data set indicated

IRR65019I • IRR65027I

by *ddname* is attempted. The data set should not be used as a RACF database.

System Action: Utility processing stops.

Problem Determination: Use the information given by both this and the preceding message to determine the proper corrective action.

IRR65019I **Output processing to *ddname* terminated due to failure during data set initialization.**

System Action: Utility processing stops.

Explanation: An error occurred while performing information retrieval, opening, writing a block, or using BSAM to write empty blocks. This message follows messages IRR65003, IRR65006, and IRR65007. See the previous message description for more information.

System Action: Processing to the database stops.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

IRR65020I **Specified options: *parm***

Explanation: The parameters specified by the user on the EXEC statement are listed.

System Action: Utility processing continues normally.

IRR65021I **Parameter error. Text beginning with '*text*' contains an undefined keyword.**

Explanation: The listed text does not start with a keyword defined to the utility.

System Action: Utility processing stops.

System Programmer Response: Check the PARM field of the EXEC statement in the JCL.

Problem Determination: Ensure that any abbreviations for keywords contain enough significant characters to make the abbreviation uniquely identifiable to the utility.

IRR65022I **Parameter error. Keyword '*keyword*' is ambiguous.**

Explanation: The utility has more than one keyword with the character string indicated by *keyword*.

System Action: Utility processing stops.

System Programmer Response: Ensure that abbreviations for keywords contain enough significant characters to make the abbreviation uniquely identifiable to the utility.

IRR65023I **Parameter error. Text beginning with '*text*' is redundant or contradictory to a previous specification.**

Explanation: Either the keyword contained in the text or its opposite form was specified previously. The utility uses the first specification of the keyword.

System Action: Utility processing stops.

System Programmer Response: Ensure that abbreviations for keywords contain enough significant characters to make the abbreviation uniquely identifiable to the utility.

Problem Determination: For a complete description of all parameters supported by this utility, see *z/OS Security Server RACF System Programmer's Guide*.

IRR65024I **Parameter error. Keyword '*keyword(value)*' contains an unacceptable value.**

Explanation: The value specified is not acceptable when associated with the keyword listed.

System Action: Utility processing stops.

System Programmer Response: See "Problem Determination."

Problem Determination: For a complete description of all parameters supported by this utility, see *z/OS Security Server RACF System Programmer's Guide*.

IRR65025I **Options in effect: *options***

Explanation: All options, including default options, in effect for the execution of this utility are listed.

System Action: Processing continues normally.

IRR65026I **Options in Effect: UNLOCKINPUT**

Explanation: UNLOCKINPUT is the only option specified for this execution of the utility.

System Action: The utility unlocks the input databases. The utility does not copy the databases.

IRR65027I **UNLOCKINPUT is the only option allowed. Processing terminated.**

Explanation: More than one option was specified. UNLOCKINPUT must be the only option requested for execution.

System Action: Utility processing stops.

System Programmer Response: Specify the UNLOCKINPUT parameter without any other option.

IRR65028I UNLOCK function requested, *ddname* already unlocked.

Explanation: The database indicated by *ddname* was unlocked before this attempt to unlock it.

System Action: Processing continues normally.

IRR65029I UNLOCK function requested, *ddname* now unlocked.

Explanation: The database indicated by *ddname* has been unlocked and is now ready for updates.

System Action: Processing continues normally.

IRR65030I UNLOCK was not successful for *ddname*

Explanation: An error occurred while attempting to unlock an input database. One of the following situations has occurred:

- The database indicated by *ddname* was not found.
- Unable to open *ddname*.
- Retrieval error for *ddname*.
- Permanent I/O error.

System Action: The database indicated by *ddname* was not unlocked. Processing stops.

System Programmer Response: To recover from the problem, do the following:

- Ensure that the DD statement is specified correctly.
- Check if *ddname* is already allocated.
- Check if there were other error messages previous to this one.

Problem Determination: If other error messages preceded this one, refer to those message explanations to determine the cause of the problem.

IRR65031I No locking parameter was specified. Processing will terminate after the following message.

Explanation: Without a locking parameter, the utility cannot continue processing.

System Action: Utility processing stops after the following message.

System Programmer Response: See following message.

IRR65032I One of the following parameters is required: LOCKINPUT, NOLOCKINPUT, or UNLOCKINPUT.

Explanation: Without a locking parameter, the utility cannot continue processing.

System Action: Utility processing stops.

System Programmer Response: Specify a locking parameter and invoke the utility again.

IRR65033I Incorrect ICB found on *ddname*. Processing will terminate.

Explanation: The ICB related to the RACF database indicated by the *ddname* in the message cannot be used by the utility.

System Action: Utility processing stops.

System Programmer Response: Check that you have specified the correct *ddname* and that it represents the RACF database you want to use. If it is, and the RACF database was not previously formatted using this utility with the PARM='NEW' specification, rerun the utility with PARM='NEW'.

Problem Determination: The validity check that caused the failure can result from an incorrect ICB value for the number of templates or BAMs, or an incorrect RBA (relative byte address). List the contents of the data set defined by the SYSRACF DD statement to determine the cause of the problem.

IRR65034I Incorrect blocksize found on *ddname*, IRRUT400 expects a blocksize of 4096. Processing will terminate.

Explanation: The DCB for the input *ddname* data set indicates a block size other than 4096. IRRUT400 only processes a data set with LRECL and BLOCKSIZE equal to 4096.

System Action: Utility processing stops.

System Programmer Response: Ensure that the data set name specified on the *ddname* DD statement has a block size of 4096.

IRR65035I Database LOCKINPUT/UNLOCKINPUT parameters are not permitted while the system is in read-only mode.

Explanation: LOCKINPUT/UNLOCKINPUT attempts to update the extend bit in the ICB. However, no database updates can be made while the system is in read-only mode.

System Action: Utility processing stops.

System Programmer Response: You can do one of the following:

- Run IRRUT400 with a parameter of LOCKINPUT/UNLOCKINPUT from another system that is not in read-only mode.
- Issue RVAR DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
- Issue RVAR NODATASHARE to change the mode of all systems to non-data sharing mode and rerun the job.

IRR65036I **A coupling facility related error occurred during database LOCKINPUT/UNLOCKINPUT processing. Utility processing has ended abnormally.**

Explanation: An error occurred when accessing the coupling facility.

System Action: IRRUT400 processing ends abnormally.

System Programmer Response: Check the SYSPRINT. Also, check the information specified in message IRRX016I, which is issued to the system console.

If the error occurred during the locking of the data sets, IRRUT400 processing has not completed. If any data sets have been locked, you should either:

- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter first, followed by the LOCKINPUT parameter.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter first, followed by the LOCKINPUT parameter.

If the error occurred during the unlocking of the data sets, you should either:

- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter.

IRR65037I **No valid *ddname* statement was found. Processing continues, but ignores this output database.**

Explanation: This message appears for each output DD statement that was not found in your JCL.

System Action: The IRRUT400 utility continues processing to identify inconsistencies between one or more input RACF databases. The range of profiles normally directed to the missing output DD statement are not written.

System Programmer Response:

- If the IRRUT400 utility ran without errors and you are running the utility to check for inconsistencies, this message is for your information only. No response is needed.
- If you meant to redistribute or copy one or more RACF databases, you need to code an output DD statement (OUTDD1, OUTDD2, and so on) for every output RACF database. For more information about allocating output databases for this utility, see *z/OS Security Server RACF System Programmer's Guide*.

IRR65038I **ICB for an empty database found on *ddname*. The database will be ignored.**

Explanation: The ICB from the RACF database identified by *ddname* was found to be valid, but the database contained no profiles.

System Action: The database identified by *ddname* is ignored by the IRRUT400 utility and processing continues. If all databases contain valid ICBs but no profiles, a return code of 16 is returned and processing stops.

System Programmer Response: Check that you have specified the correct DDNAME and that it represents the RACF database you want to use.

Internal reorganization of aliases utility (IRRIRA00) messages

IRR66000I **Invalid input to message writing routine attempting to write message number *message-number*.**

Explanation: This is an error internal to the utility. The specified message number was not found.

System Action: System processing continues. Utility processing may or may not continue.

Programmer Response: Record the specified message number and contact your IBM support center.

IRR66001I **Unable to establish recovery environment. Processing ended.**

Explanation: An estae environment could not be established.

System Action: Utility processing stops.

Programmer Response: Report this problem to your system programmer.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, contact the IBM support center.

IRR66002I Unable to run IRRIRA00. RACF is not active.

Explanation: RACF is not installed on the system, or it is inactive.

System Action: Utility processing stops.

Programmer Response: Report this problem to your system programmer.

System Programmer Response: Ensure that RACF is properly installed, and is active on the system.

IRR66003I Unable to run IRRIRA00. Backup RACF database is partially inactive.

Explanation: The backup RACF database contains multiple data sets. Some data sets are currently active, and some inactive. The utility cannot create a valid backup database in this state.

System Action: Utility processing stops.

Programmer Response: Report this problem to your system programmer.

System Programmer Response: Issue RVARY to activate or inactivate all data sets in the backup RACF database and rerun the job.

IRR66004I RACF database cannot be updated. System is in read-only mode.

Explanation: IRRIRA00 must update the RACF database to change the current stage. However, no database updates can be made because the system is currently in read-only mode.

System Action: Utility processing stops.

Programmer Response: Run IRRIRA00 from another system that is not in read-only mode, or report the problem to your system programmer.

System Programmer Response: You can do one of the following:

- Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
- Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode and rerun the job.

IRR66005I A coupling facility related error occurred. Utility processing has ended abnormally.

Explanation: An error occurred when accessing the coupling facility.

System Action: Utility processing stops.

Programmer Response: Check the SYSPRINT for related error messages and report them to your system

programmer. Run IRRIRA00 from another system in the data sharing group.

System Programmer Response: Check for related console and syslog messages and perform any actions associated with the responses for those messages.

IRR66006I Stage *stage-number* requested. Database already at requested stage.

Explanation: The RACF database was already at the stage specified by the stage parameter.

System Action: Utility processing stops.

Programmer Response: If you want to move the system to the next stage, correct the value of the stage parameter and run the job again.

IRR66007I Backup RACF database not converted to stage *stage-number*. It is not active.

Explanation: The RACF primary database was converted to the stage requested, but the backup RACF database was not converted because it is not currently active.

System Action: Utility processing continues.

Programmer Response: Copy the primary RACF database to the backup before activating the backup database.

IRR66008I *abend-code* abend during utility processing.

Explanation: The specified abnormal termination occurred during the execution of the utility.

System Action: Utility processing stops.

Programmer Response: Use the indicated abend code and any previous messages issued to determine the appropriate action. Rerun the job after correcting the problem.

IRR66009I Last entry processed successfully was *entry-name* in class *class-name*.

Explanation: Because of an error identified by a preceding message, no further processing of this database will be attempted.

System Action: Utility processing stops.

Programmer Response: Correct the error indicated by any previous messages issued and rerun the job.

IRR66010I Parameter error. Unsupported stage value specified.

Explanation: The stage parameter specified a value that is not in the supported range.

System Action: Utility processing stops.

IRR66011I • IRR66020I

Programmer Response: Correct the stage parameter and run the job again.

IRR66011I Parameter error. Undefined parameter specified.

Explanation: A parameter was specified that is not recognized by the utility.

System Action: Utility processing stops.

Programmer Response: Correct the specified parameter and run the job again.

IRR66012I Parameter error. Converting from stage *current-stage-number* to stage *specified-stage-number* is not allowed.

Explanation: The utility cannot convert the database from its current stage to the stage specified by the stage parameter.

System Action: Utility processing stops.

Programmer Response: Correct the value specified for the stage parameter and run the job again.

IRR66013I Parameter error. No closing parenthesis found.

Explanation: The utility did not find a closing parenthesis in the parameter specification.

System Action: Utility processing stops.

Programmer Response: Correct the parameter specification and run the job again.

IRR66014I Parameter error. No stage value specified.

Explanation: The utility did not find a value specified for the stage parameter.

System Action: Utility processing stops.

Programmer Response: Specify a value for the stage parameter, or omit the parameter to display the current stage, and run the job again.

IRR66015I Parameter error. Extraneous text follows stage parameter.

Explanation: The utility found unexpected text following the value specified for the stage parameter.

System Action: Utility processing stops.

Programmer Response: Correct the parameter specification and run the job again.

IRR66016I Unexpected RACF manager return code [deleting | updating] entry *entry-name* in class *class-name*. Return code *return-code*. Reason code *reason-code*.

Explanation: While altering the RACF database, a return code was returned by the RACF manager indicating that an error was encountered.

System Action: Utility processing stops.

Programmer Response: Use the decimal return code and reason code to determine the cause of the problem. *z/OS Security Server RACF Macros and Interfaces* contains the ICHEINTY return and reason codes. Correct the problem and run the job again.

IRR66017I The system is currently operating in stage *stage-number*.

Explanation: The RACF RCVT indicates that the system is currently operating in the stage indicated. This is a status message only.

System Action: None.

Programmer Response: If you want to move the system to the next stage, rerun the utility with the stage parameter specified.

IRR66018I Stage *stage-number* requested. Database now at requested stage.

Explanation: The RACF database was successfully converted to the stage specified by the stage parameter.

System Action: None.

IRR66019I Unable to open *dsname*.

Explanation: The utility was unable to open the RACF data set *dsname* to process the ICB.

System Action: Utility processing stops.

Programmer Response: Check for other errors related to the DASD volume on which the data set resides, correct the problem and rerun the job.

IRR66020I [Allocation | Deallocation] for *dsname* failed with error code *code*.

Explanation: The utility issued a dynamic allocation request (SVC 99) to allocate or deallocate the RACF data set *dsname*. However, the return code from dynamic allocation was unexpected.

Programmer Response: Check the return code from the SVC 99 in *z/OS MVS Authorized Assembler Services Guide* and correct the problem. If the error took place during deallocation processing, the stage value may already have been incremented. Rerun the

job to check or increment the stage value.

IRR66021I **Unexpected RACF manager return code attempting to locate next entry after entry** *entry-name* **in class** *class-name*. **Return code** *return-code*.
Reason code *reason-code*.

Explanation: While reading the RACF database, a return code was returned by the RACF manager indicating that an error was encountered.

System Action: Utility processing stops.

Programmer Response: Use the decimal return code and reason code to determine the cause of the problem. *z/OS Security Server RACF Macros and Interfaces* contains the ICHEINTY return and reason codes. Correct the problem and run the job again.

IRR66022I **Unable to run IRRIRA00. Templates are downlevel and do not support alias index entry creation.**

Explanation: IRRIRA00 has detected that the level of templates currently in use does not support the creation of alias index entries.

System Action: Utility processing stops.

Programmer Response: Run IRRMIN00 with PARM=UPDATE to update the templates to the correct level. Ensure that the correct RACF database has been specified. After you run IRRMIN00 you will need to re-IPL before the template changes become effective. After you re-IPL, run the job again.

RACF database unload utility (IRRDBU00) and RACF SMF data unload utility (IRRADU00) messages

IRR67000I **Incorrect input to message writing routine attempting to write message number** *message-number*

Explanation: This is an error internal to the utility. The specified message number was not found.

System Action: Utility processing continues.

Problem Determination: Record the specified message number and contact your IBM support center.

IRR67001I **Unable to establish recovery environment. Processing terminated.**

Explanation: An ESTAE environment could not be established.

System Action: Utility processing stops.

System Programmer Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

Problem Determination: See "System Programmer Response."

IRR67004I *utility-name* **UNSUCCESSFUL: CANNOT OPEN SYSPRINT.**

Explanation: The sysprint DCB could not be opened in order to enable messages to be printed.

System Action: Utility processing stops.

Problem Determination: Ensure that SYSPRINT has been allocated in the JCL.

Note: This is a WTO with routing code 11.

IRR67005I **RACF is not active.**

Explanation: RACF is not installed on system or it is inactive.

System Action: Utility processing stops.

System Programmer Response: Ensure that RACF is properly installed on system.

Problem Determination: Contact your IBM support center if this problem recurs.

IRR67006I **RACF is not at appropriate release level.**

Explanation: RACF is installed, but is not at least version 1.9.0.

System Action: Utility processing stops.

System Programmer Response: Install RACF 1.9.0 or later on your system.

Problem Determination: Contact your IBM support center if this problem recurs.

IRR67007I **The blocksize was taken from DD *ddname* and the data set was closed.**

Explanation: The block size was successfully read from the specified database.

System Action: Utility processing continues.

IRR67008I **The blocksize was taken from DD *ddname* but an error occurred while closing the data set.**

Explanation: The block size was successfully read from the specified data set, but this data set could not be closed.

System Action: Utility processing stops.

Problem Determination: This message is accompanied by messages issued by DFP. Follow the problem determination procedure for the DFP messages. These are contained in the MVS system messages document.

IRR67010I **Specified option:** *option*

Explanation: The parameter specified with the PARM= field in the EXEC statement is listed here. The parameters NOLOCKINPUT, LOCKINPUT and UNLOCKINPUT can be abbreviated to a minimum of N,L and U, respectively. If no option is specified, message IRR67021I is issued.

System Action: Utility processing continues.

IRR67011I **Parameter error. Text beginning with '*text.*' contains an undefined keyword.**

Explanation: An incorrect parameter was passed to the utility.

System Action: Utility processing stops.

System Programmer Response: Ensure that only one of the following was specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

Problem Determination: Check the PARM= field of the EXEC statement.

IRR67012I **Parameter error. Text beginning with 'text.' is longer than valid keywords.**

Explanation: An incorrect parameter was passed to the utility.

System Action: Utility processing stops.

System Programmer Response: Ensure that only one of the following was specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

Problem Determination: Check the PARM= field of the EXEC statement.

IRR67013I **Option in effect: option**

Explanation: The full text of the option that the utility processes (based on the PARM operand of the EXEC statement) is displayed here.

System Action: Utility processing continues.

IRR67016I **RACF unable to build an ACEE. RACINIT return code is return-code.**

Explanation: The accessor environment element (ACEE) could not be built for either the input or output RACF database.

System Action: Utility processing stops.

System Programmer Response: Be sure that RACF is properly installed on system.

Problem Determination: Record RACINIT return code and this message ID. Contact your IBM support center.

IRR67020I **Parameter error. Text 'text' is incorrect. Only one parameter may be specified.**

Explanation: More than one parameter was passed to the utility on the EXEC statement.

System Action: Utility processing stops.

System Programmer Response: Ensure that only one of the following was specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

Problem Determination: Check the PARM= field in the EXEC statement.

IRR67021I **No parameter specified. One of the following is required: LOCKINPUT, NOLOCKINPUT, or UNLOCKINPUT.**

Explanation: No parameters were passed to the utility.

System Action: Utility processing stops.

System Programmer Response: Ensure that one of the following is specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

Problem Determination: Check the PARM= field in the EXEC statement.

IRR67060I ***** Profile processing not started *****

Explanation: No database processing was attempted because of a previous failure in setting up the utility.

System Action: Utility processing stops.

System Programmer Response: Ensure that the proper initializations were made before executing the utility. Rerun the utility after correcting errors identified in previous messages.

Problem Determination: Use the messages displayed before this one to help determine what the specific problem is.

IRR67090I **Unexpected RACF manager return code while reading the data base. The next message contains diagnostic information.**

Explanation: While attempting to read the RACF database, a return code was returned by RACF indicating an error during the READ operation.

System Action: Utility processing stops.

Problem Determination: The next message, IRR67092I, contains the return code, the reason code, and the entry that was being processed. Use this information and information about ICHEINTY return codes from *z/OS Security Server RACF Macros and Interfaces* to determine the proper action.

IRR67092I **Return code: return-code reason code: reason-code entry name: entry-name.**

Explanation: This message is issued after IRR67090I. This message contains the return code, reason code, and entry name that were returned from the failing request. A blank entry name indicates that the utility was processing the first entry in the profile type.

System Action: Utility processing stops.

Problem Determination: Use the return code and reason code to determine the cause of the problem. *z/OS Security Server RACF Macros and Interfaces* contains these ICHEINTY return and reason codes.

IRR67093I **Processing profile-type profiles.**

Explanation: This is an informational message identifying the type of profiles that the utility is now processing.

System Action: Processing continues.

IRR67120I **abend-code abend during utility processing. Reason code reason-code.**

Explanation: A system abend occurred during utility processing.

IRR67121I • IRR67153I

System Action: Utility processing continues with recovery procedures.

Problem Determination: For more information about the indicated abend, see *z/OS MVS System Codes*.

IRR67121I The module in control at time of abend was *module-name*.

Explanation: The internal module which was in control at the time of the abend is listed here for debugging purposes.

System Action: Utility processing continues with recovery procedures.

Problem Determination: This message is accompanied by message IRR67120I. If the problem recurs after following the problem determination for the above message number, then record all information provided by these two messages and contact your IBM support center.

IRR67122I * Utility ESTAE error routine in control. *****

Explanation: The recovery procedure for the utility is now processing.

System Action: Recovery processing begins.

IRR67123I Profile processing DID finish before the abend. Output should be complete.

Explanation: The recovery routine has determined that the abend specified in message IRR67120I occurred after all profiles had been processed. The output file should be complete. The abend must have occurred during resource cleanup.

System Action: Recovery processing continues.

Problem Determination: Verify that the utility completed, using the IRRUT200 verification utility.

IRR67124I Profile processing DID NOT finish before the abend. Output is NOT complete.

Explanation: The recovery routine has determined that the abend specified in message IRR67120I occurred before the utility completed.

System Action: Recovery processing continues.

System Programmer Response: The output file was too small. Allocate a bigger output file and rerun the utility.

IRR67125I Utility ESTAE error routine will now attempt clean-up processing.

Explanation: An attempt will be made to free all main storage that was used by the utility.

Note: If message IRR67124I was issued before this message, and you specified the LOCKINPUT parameter to lock the databases, the databases remain unlocked unless they were already locked before the utility was invoked.

IRR67150I Processing *count* RACF data set(s).

Explanation: The database utility expects to process the indicated number of RACF data sets. This number is taken from the system data set name table (ICHRDSNT).

System Action: Processing continues normally.

IRR67151I LOCKINPUT parameter specified. DD *ddname* is now locked.

Explanation: The LOCKINPUT parameter was specified in the input specifications for the utility. The RACF database is locked. Others cannot write to the RACF database until the database is unlocked. To unlock the database, use the IRRUT400 or IRRDBU00 utility with the UNLOCKINPUT parameter specified.

System Action: Processing continues normally.

IRR67152I LOCKINPUT parameter specified. DD *ddname* was already locked. Processing continues with this DDNAME.

Explanation: The LOCKINPUT parameter was specified in the input specifications for the utility, but the specified RACF database was already locked. Others cannot write to the RACF database until the database is unlocked. To unlock the database, use the IRRUT400 or IRRDBU00 utility with the UNLOCKINPUT parameter specified.

System Action: Processing continues normally.

IRR67153I Unexpected DD statement *ddname* found.

Explanation: You specified more DD statements than the RACF utility expected.

System Action: Processing stops.

System Programmer Response: Ensure that the number of INDDx statements is the same as indicated by message IRR67150I.

IRR67154I Blocksize is incorrect for *data-set-name* on volume *volume*.

Explanation: The block size specified for the indicated data on the indicated volume is incorrect.

System Action: Processing stops.

System Programmer Response: Omit the BLKSIZE parameter on the DD statement, or specify the correct value for the indicated RACF database.

IRR67155I INDD1 is neither a primary nor backup data set. No other input data set can be a primary or backup data set.

Explanation: The utility is processing a database that is not being used by RACF as either a primary or backup database.

System Action: Processing continues normally.

System Programmer Response: Make sure that any updates to the primary or backup database are incorporated in the database that is produced by the utility.

IRR67156I DD *ddname* specifies a primary or backup data set, but a non-primary or non-backup data set was expected.

Explanation: The DD statement for INDD1 specifies a nonprimary or nonbackup data set. Therefore, the utility expects all data sets to be nonprimary or nonbackup data sets. However, the *ddname* indicated in the message specifies a primary or backup data set.

System Action: The utility stops processing.

System Programmer Response: Correct the DD statements and rerun the job.

IRR67157I DD *ddname* is not a primary data set. The following message shows the expected primary data set.

Explanation: The DD statement for INDD1 specifies a primary data set. Therefore, the utility expects all data sets to be primary data sets. However, the *ddname* indicated in the message specifies a nonprimary data set.

System Action: Processing stops.

System Programmer Response: Correct the DD statements and rerun the job.

IRR67158I DD *ddname* is not a backup data set. The following message shows the expected backup data set.

Explanation: The DD statement for INDD1 specifies a backup data set. Therefore, the utility expects all data sets to be backup data sets. However, the *ddname*

indicated in the message specifies a nonbackup data set.

System Action: Processing stops.

System Programmer Response: Correct the DD statements and rerun the job.

IRR67159I The data set specified for INDD1 is primary or back up, but it is not the first entry in ICHRDSNT.

Explanation: The DD statement for INDD1 specifies a data set that is either primary or backup. Therefore, INDD1 must be the first data set listed in the data set name table (ICHRDSNT). The *ddname* indicated in the message specifies a data set that is either primary or backup and not the first entry in ICHRDSNT.

System Action: Processing stops.

System Programmer Response: Correct the DD statements, and rerun the job.

IRR67160I Internal error in the utility.

Explanation: An error occurred in the processing of the utility.

System Action: Processing stops.

System Programmer Response: Report this message to your IBM support center. Please include the following information: Interpreted JCL and SYSOUT.

IRR67161I Failed write for DD *ddname*.

Explanation: An error occurred while writing to the indicated data set.

System Action: Processing stops.

System Programmer Response: This could be caused by a problem with the *ddname* indicated in the message.

Problem Determination: This message is accompanied by messages issued by DFP. Follow the problem determination procedure for the DFP messages.

IRR67162I Dataset is *data-set-name* on volume *volume*.

Explanation: This message identifies a RACF database described in an earlier message. If the device containing *data-set-name* has been dynamically reconfigured from the system, *NA replaces the *volume* information in the message.

System Action: See "System Action" for the earlier message.

IRR67163I INDD1 is a primary data set. All input data sets must be primary data sets.

Explanation: The DD statement for INDD1 specifies a primary data set. Therefore, the utility expects all data sets to be primary data sets.

System Action: Processing continues normally.

IRR67164I INDD1 is a backup data set. All input data sets must be backup data sets.

Explanation: The DD statement for INDD1 specifies a backup data set. Therefore, the utility expects all data sets to be backup data sets.

System Action: Processing continues normally.

IRR67165I The RACF data set name table (ICHRDSNT) indicates that there are *nn* RACF data sets, but only one was specified.

Explanation: The utility can process either your entire RACF database or a single data set of a multi-data set database. The utility has determined that you are processing a single data set from a multi-data set database.

System Action: Utility processing continues.

System Programmer Response: You may ignore the count in IRR67150I if you are attempting to process a single data set from a multi-data set database.

IRR67166I Processing continues using as input the data set specified as INDD1.

Explanation: The utility can process either your entire RACF database or a single data set of a multi-data set database. The utility has determined that you are processing a single data set from a multi-data set database.

Be sure to examine the output of the utility for any occurrences of the IRR67092I message with a return code of X'00000012' and reason code of X'00000000', which can occur when a user profile is contained in a separate database from its connect profiles. This can happen if your range table splits the database at a boundary between user profiles and connect profiles.

Note: This can only occur if your range table splits the database with a value that has two consecutive null values, such as X'C10000C1'. If your range table has such a value, you must process all parts of your database in one execution of the utility.

IRR67167I Multiple OUTDD statements were specified, but only one INDD was specified.

Explanation: The number of INDDx statements must be identical to the number of OUTDDx statements.

System Programmer Response: Execute the utility specifying the same number of INDDx and OUTDDx statements.

System Action: Utility processing stops.

IRR67168I Multiple INDD statements were specified, but only one OUTDD was specified.

Explanation: The number of INDDx statements must be identical to the number of OUTDDx statements.

System Programmer Response: Execute the utility specifying the same number of INDDx and OUTDDx statements.

System Action: Utility processing stops.

IRR67169I Database LOCKINPUT/UNLOCKINPUT parameters are not permitted while the system is in read-only mode.

Explanation: LOCKINPUT/UNLOCKINPUT attempts to update the extend bit in the ICB. However, no database updates can be made while the system is in read-only mode.

System Action: Utility processing stops.

System Programmer Response: You can do one of the following:

- Run IRRDBU00 with a parameter of LOCKINPUT/UNLOCKINPUT from another system that is not in read-only mode.
 - Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
 - Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode and rerun the job.
-

IRR67180I Unable to open *data-set-name* associated with DD *ddname*.

Explanation: An error occurred while attempting to open the specified database.

System Action: Processing stops.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the data set resides.

IRR67181I Information retrieval for DD *ddname* failed with error code *error-code*.

Explanation: The utility issued a dynamic allocation request (SVC 99) for information about the *ddname* indicated in the message. However, the return code from dynamic allocation was unexpected.

System Programmer Response: See “Problem Determination.”

Problem Determination: Check the return code from the SVC 99 in *z/OS MVS Programming: Authorized Assembler Services Guide*.

System Action: Processing stops.

IRR67182I *data-set-name* associated with DD *ddname* has been successfully opened.

Explanation: The specified data set is now open so that the utility can read from it or write to it.

System Action: Processing continues normally.

IRR67183I DD *ddname* not found.

Explanation: The specified DD was expected, but not found. If you are processing a single data set of a multi-data set database, you can ignore this message for INDD2.

System Action: If the *ddname* is INDD2, processing continues. For any other *ddname*, processing stops.

System Programmer Response: Ensure that the number of INDDx statements is the same as indicated by message IRR67150I.

Problem Determination: Check the job's DD statements to verify that the correct number of INDDs and OUTDDs are allocated.

IRR67240I DD *ddname* could not be unlocked because of a write failure.

Explanation: An error occurred while attempting to unlock the specified input database.

System Action: Utility processing stops.

System Programmer Response: To recover from the problem, consider doing the following:

- Ensure that the DD statement is correct.
- If you are processing primary databases, switch to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information on recovering from the problem, see the section on RACF database recovery in *z/OS Security Server RACF System Programmer's Guide*. Pay particular attention to the section on failures during I/O operations on the RACF database.

Problem Determination: Other messages might have been issued for this problem. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, which reports a return code from the RACF manager.

IRR67241I Unlock was successful. DD *ddname* is now unlocked.

Explanation: The RACF database indicated by the *ddname* can now be updated.

System Action: Utility processing continues.

IRR67242I DD *ddname* is already unlocked.

Explanation: You asked to unlock a database that is already unlocked.

System Action: Utility processing continues.

IRR67243I DD *ddname* could not be unlocked because of a read failure.

Explanation: An error occurred while attempting to read the specified input data set's ICB to determine its lock status.

System Action: Utility processing stops.

System Programmer Response: To recover from the problem, consider doing the following:

- Ensure that the DD statement is correct.
- If you are processing primary databases, switch to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information on recovering from the problem, see the section on RACF database recovery in *z/OS Security Server RACF System Programmer's Guide*. Pay particular attention to the section on failures during I/O operations on the RACF database.

Problem Determination: Other messages might have been issued for this problem. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, which reports a return code from the RACF manager.

IRR67244I Unlock processing was attempted in read-only mode, which is not allowed. Data sets may still be locked.

Explanation: LOCKINPUT processing began in either non-data sharing mode or data sharing mode and may have locked data sets. At the start of the unlock portion of LOCKINPUT processing, it was found that the system is in read-only mode.

System Action: Utility processing ends abnormally.

IRR67270I • IRR67333I

System Programmer Response: You can do one of the following:

- Run IRRDBU00 with a parameter of UNLOCKINPUT from another system that is not in read-only mode.
- Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
- Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode and rerun the job.

IRR67270I *error-message-text on ddname while attempting a request of a block at RBA rba*

Explanation: The indicated error occurred while attempting a BDAM read (READ) or BDAM write (WRITE).

System Action: The ddname of the file on which the error occurred is listed, along with the RBA (relative byte address) of the byte being accessed.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the database resides.

IRR67271I **A coupling facility related error occurred during database LOCKINPUT/UNLOCKINPUT processing for ddname.**

Explanation: While writing the ICB to the coupling facility, the utility detected an error. The ddname of the file on which the error occurred is listed.

System Action: Utility processing ends abnormally.

System Programmer Response: Check the SYSPRINT. Also, check the information specified in message IRRX016I, which is issued to the system console.

If the error occurred during the locking of the data sets, they have not been unloaded. If any data sets have been locked, you should either:

- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter first, followed by the LOCKINPUT parameter.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter first, followed by the LOCKINPUT parameter.

If the error occurred during the unlocking of the data sets, you should either:

- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter.

- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter.

IRR67330I **RACF manager load module module-name could not be loaded.**

Explanation: An error occurred while attempting to load the specified manager load module.

System Action: Utility processing stops.

Problem Determination: Ensure that RACF is properly installed on the system.

IRR67331I **Unable to obtain the number of records per track for dsname DD ddname.**

Explanation: An error occurred in attempting to read the number of records per track for the specified RACF database.

System Action: Utility processing stops.

Problem Determination: Check for other errors related to the disk pack on which the database resides. Make sure the correct ddname and data set name were specified.

IRR67332I **RACF data set dsname DD ddname cannot be used - incorrect ICB.**

Explanation: An error occurred while validating the ICB (inventory control block) of the specified RACF database.

System Action: Utility processing stops.

System Programmer Response: Ensure that the specified database is properly initialized.

Problem Determination: This error message is produced if any of the following is true:

- The initialization routine, IRRMIN00, failed to completely initialize the RACF database or was never run against it.
- No block availability masks (BAMs) exist for this database.
- The RACF templates are not at least version 1.9 or later.
- The relative byte addresses (RBAs) for this database are incorrect.

IRR67333I **RACF unable to locate module-name in LPA.**

Explanation: RACF searched the link pack area and could not locate the specified module necessary for RACF processing. Processing cannot continue.

System Action: Utility processing stops.

System Programmer Response: Ensure that the system parameters MLPA and LNK have been specified correctly. Make sure that the system has been installed correctly.

IRR67335I I/O error occurred while trying to read the ICB for *dsname* DD *ddname*.

Explanation: The ICB (inventory control block) for the specified RACF database could not be read.

System Action: Utility processing stops.

System Programmer Response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the database resides.

IRR67336I I/O error occurred while trying to update the ICB for *dsname* DD *ddname*.

Explanation: The ICB could not be written back to the specified output database after it had been updated with the necessary RACF options.

System Action: Utility processing stops.

System Programmer Response: Specify a SYSUDUMP control card on the JCL used to invoke the utility so that the register contents can be viewed. Register 15 contains the status indicators and a pointer to the error analysis routine.

IRR67402I Database unload utility has successfully finished processing.

Explanation: No errors were encountered while unloading the database.

System Action: Utility processing stops. If the LOCKINPUT parameter was specified, the input databases are unlocked.

IRR67403I Database unload utility completed unsuccessfully.

Explanation: An error was encountered during utility processing.

System Action: If the error is an index read error, utility processing stops. If the error is a non-index read error, utility processing continues and the failing profile is flagged. The RACF manager return and reason codes are issued. If the LOCKINPUT parameter was in effect and the input databases were not locked before you invoked the unload utility, these databases are unlocked before the utility stops.

Problem Determination: This message is accompanied by other error messages, which can be used to help pinpoint what caused the unload utility to stop.

IRR67417I RACF created a down level ACEE. Database unload requires at least a level 2 ACEE.

Explanation: The accessor environment element (ACEE) must be at least level 2.

System Action: Utility processing stops.

System Programmer Response: Ensure that RACF version 1.9.0 or later is properly installed on the system.

Problem Determination: If this message recurs, contact your IBM support center.

IRR67422I Incorrect blocksize specified for INDD1. The blocksize must be 4096.

Explanation: The data set that is specified as INDD1 must have a blocksize of 4096. The data set specified as INDD1 had a blocksize of other than 4096.

System Action: Utility processing stops.

System Programmer Response: Specify a valid data set as INDD1.

Problem Determination: Check the INDD1 DD statement.

IRR67423I Open failed for OUTDD.

Explanation: An error occurred while attempting to open the output data set.

System Action: Utility processing stops.

Problem Determination: Ensure that OUTDD is specified.

IRR67460I * Profile unloading not started *****

Explanation: Database unloading was not attempted because of a prior failure in setting up the utility.

System Action: Utility processing stops.

System Programmer Response: Ensure that the proper initializations were made before executing the unload utility. Rerun the utility after correcting errors identified in previous messages.

Problem Determination: This message is displayed after an error has been encountered. Use the messages before this one to help determine what the specific problem is.

IRR67494I *profile-count profile-type [class-name] profile(s)* have been unloaded.

Explanation: This is an informational message identifying the number and the type of the profiles that the Database Unload Utility has just unloaded. The *class-name* is only displayed for general resource profiles.

IRR67495I • IRR67551I

System Action: Processing continues.

IRR67495I * Unloading not completed. *****

Explanation: The Database Unload Utility detected an error condition. Output is not complete.

System Action: Processing halts.

Problem Determination: Examine the previous messages.

IRR67500I The Field Definition Table (FDT) and the ACTN area do not match. The unknown field is ccccccc.

Explanation: An internal error has occurred.

Severity: Error

User Response: Call the IBM support center.

System Action: Utility processing stops.

IRR67520I Unable to establish recovery environment. Processing terminated.

Explanation: An ESTAE environment could not be established.

System Action: Utility processing stops.

User Response: Ensure that RACF and the operating system are properly installed. If they are, report this message (and its message ID) to your IBM support center.

IRR67522I Open failed for OUTDD.

Explanation: An error occurred while attempting to open the output data set.

System Action: Utility processing stops.

User Response: Ensure that OUTDD is specified.

IRR67524I A pre-RACF 1.9 record was encountered in the input stream. The record is ignored.

Explanation: The input contains a record created by an unsupported version of RACF. Because this utility can process only SMF records that were created by RACF Version 1.9.0 or later, the record is ignored. Message IRR67581I identifies the failing record in more detail.

System Action: Utility processing continues.

IRR67534I IRRADU00 UNSUCCESSFUL: CANNOT OPEN SDUPRINT.

Explanation: IRRADU00 could not open the required sysprint file ADUPRINT. This message is issued via a write-to-operator (WTO) request.

System Action: Utility processing stops.

User Response: Allocate the file ADUPRINT before executing the utility.

IRR67540I The LRECL of the output data set allocated to OUTDD has been changed from *original_lrecl* to *new_lrecl*.

Explanation: The logical record length (LRECL) of the output data set was *original_lrecl*, which was smaller than that which is required by the utility. The utility has set the LRECL of the output data set to *new_lrecl*.

System Action: Utility processing continues.

IRR67541I The BLKSIZE of the output data set allocated to OUTDD has been changed from *original_block_size* to *new_block_size*.

Explanation: The block size of the output data set was *original_block_size*, which was smaller than that which is required by the utility. The utility has set the BLKSIZE of the output data set to *new_block_size*. Note that the block size of the output data set must be at least 4 bytes larger than the logical record length.

System Action: Utility processing continues.

IRR67550I *abend_code* abend during utility processing. Reason code *rsncode*.

Explanation: A system abend occurred during utility processing.

System Action: Utility processing continues with the recovery procedure.

User Response: For more information about the indicated abend, see an MVS/ESA system codes documentation.

IRR67551I The module in control at time of abend was *module_name*.

Explanation: The internal module that was in control at the time of the abend is listed here for debugging purposes.

System Action: Utility processing continues with the recovery procedure.

User Response: This message is accompanied by message number IRR67550I. If the problem recurs after following the problem determination for the above message number, then record all the information provided by these two messages and contact your IBM support center.

IRR67552I * Utility ESTAE error routine in control. *****

Explanation: The recovery procedure for the utility is now running.

System Action: Recovery processing begins.

IRR67580I Unexpected relocate section found in type *record_type* record for event code *event_code*/*event_code_qualifier*. The relocate number is *relocate_number*.

Explanation: This error message indicates that the SMF record being processed contained an unexpected relocate section. The type of the record is *record_type*. The unexpected relocate section is *relocate_number*. *Event_code*/*event_code_qualifier* are the event code and event code qualifier for the record.

Message IRR67581I identifies the failing record in more detail.

System Action: Utility processing continues.

User Response: Perform these steps:

1. Obtain a hexadecimal print of the failing record from the input supplied to the utility. You can use the MVS utilities IDCAMS or DITTO or their equivalent for this.
 2. Compare the relocate sections that you find in the record with the relocate sections that are defined as valid for the specific event code. You can find a list of event codes, relocate sections, and the components that created the record, in *z/OS MVS System Management Facilities (SMF) and z/OS Security Server RACF Macros and Interfaces*.
 3. Contact the IBM support center.
-

IRR67581I The failing record, *relative_record*, was created on *date* at *time* for user *userid* in group *groupid* on system *smf_id*.

Explanation: This message identifies the failing record for which message IRR67580I or message IRR67524I was created.

System Action: Utility processing continues.

User Response: Use this information to locate the failing record so that you can find the failing profile. *Relative_record* might be useful when using print utilities such as IDCAMS and DITTO, which allow the specification of a relative record number. See *z/OS DFSMS Access Method Services for Catalogs* for more information on these utilities.

Note that the relative record number is the number of the record as it was passed to IRRADU00. This number may differ from the relative record number in the data set that was input to IFASMFDP if the IFASMFDP control statements suppressed the processing of some record type. See *z/OS MVS System Management*

Facilities (SMF) for more information on the control statements for IFASMFDP.

IRR67582I The data associated with the relocate section is "*relocate_data*" and has a length of *relocate_data_length*.

Explanation: This message describes the data (*relocate_data*) associated with the unexpected relocate section that was identified in message IRR67580I. The length associated with the relocate section is shown as *relocate_data_length*. If the length of the data exceeds 16 bytes, only the first 16 bytes are shown in the message.

System Action: Utility processing continues.

IRR67650I SMF data unload utility has successfully completed.

Explanation: IRRADU00 has successfully finished processing.

IRR67651I SMF data unload utility has not successfully completed.

Explanation: IRRADU00 found one or more errors during processing.

User Response: Review the messages produced by both IRRADU00 and the system. Take the actions indicated in the messages.

IRR67652I The utility processed *record_count* SMF type *record_type* records.

Explanation: This informational message describes the number of records processed (*record_count*) for each type of record (*record_type*) that the utility processes.

System Action: Utility processing continues.

IRR67653I The utility bypassed *record_count* SMF records not related to IRRADU00.

Explanation: This informational message tells you how many records (*record_count*) that were bypassed by the utility. The utility processes these SMF record types:

- type 30 ("Job initiation")
- type 80 ("RACF processing")
- type 81 ("RACF initialization")
- type 83 ("RACF auditing data sets")

Refer to the *z/OS MVS System Management Facilities (SMF) and z/OS Security Server RACF Macros and Interfaces* for a complete description of these records.

System Action: Utility processing continues.

RACF remove ID utility (IRRRID00) messages

IRR68001I No IDs were found in the SYSIN data set. A search for all residual references is being performed.

Explanation: Since you did not specify one or more IDs for IRRRID00 to search for, a search is being made for all residual references. Possible causes of IRRRID00 not finding any IDs are: SYSIN was not allocated correctly, SYSIN was allocated to DUMMY, or SYSIN was not specified.

System Action: Utility processing continues.

User Response: If you intended to search for all residual references, no action is required. Otherwise, correct the SYSIN statements and submit the job again.

IRR68002I IRRRID00 found *count* records with inconsistent IDs.

Explanation: IRRRID00 found the indicated number of places in the database in which an ID value was used inconsistently. IRRRID00 verifies that in those places where only a user ID is valid, only a user ID is used. Similar verification is performed for group IDs. This message tells you how many times IRRRID00 found an ID value that was used improperly. Each occurrence of the improper ID is flagged with messages IRR68017I and IRR68018I.

System Action: Utility processing continues.

IRR68003I DDNAME *ddname* did not open.

Explanation: The required DDNAME *ddname* could not be opened.

System Action: Utility processing stops with a decimal return code of 16.

User Response: Correct the JCL and submit the job again.

IRR68004I IRRRID00 found *count* references.

Explanation: IRRRID00 detected the indicated number of references to the user IDs and group IDs you supplied.

System Action: Utility processing continues.

IRR68005I IRRRID00 UNSUCCESSFUL: CANNOT OPEN SYSPRINT.

Explanation: IRRRID00 could not open the required SYSPRINT file. This message is issued via a write-to-programmer (WTP) request.

System Action: Utility processing stops, with decimal return code 20.

User Response: Allocate the SYSPRINT file before

running the utility. Correct the JCL and submit the job again.

IRR68006I The LRECL of the output data set allocated to OUTDD has been changed from *original_lrecl* to *new_lrecl*.

Explanation: The logical record length (LRECL) of the output data set was *original_lrecl*, which was smaller than required by the utility. The utility has set the LRECL of the output data set to *new_lrecl*.

System Action: Utility processing continues.

IRR68007I The BLKSIZE of the output data set allocated to OUTDD has been changed from *original_block_size* to *new_block_size*.

Explanation: The block size of the output data set was *original_block_size*, which was smaller than required by the utility. The utility has set the BLKSIZE of the output data set to *new_block_size*. Note that the block size of the output data set must be at least 4 bytes larger than the logical record length.

System Action: Utility processing continues.

IRR68008I *** Utility ESTAE error routine in control. ***

Explanation: The recovery procedure for the utility is now processing. This message is accompanied by message number IRR68009I and IRR68010I.

System Action: Recovery processing begins and utility processing stops with a decimal return code of 16.

User Response: Follow the user responses specified in messages IRR68009I and IRR68010.

IRR68009I *abend_code* abend occurred during utility processing. The reason code is *reason_code*.

Explanation: An abend occurred during utility processing. This message is accompanied by message numbers IRR68008I and IRR68010I. *abend_code* is a six-hexadecimal-character string in which the first three hexadecimal characters are the system abend code and the last three hexadecimal characters are the user abend code. *reason_code* is also a hexadecimal character string.

System Action: Utility processing continues with the recovery procedure.

User Response: For more information about the indicated abend, see *z/OS MVS System Codes* and correct the problem.

IRR68010I The module in control at the time of the abend was *module_name* - *text*.

Explanation: The internal module that was in control at the time of the abend is listed here for debugging purposes. The *text* displayed describes the last function attempted by the indicated module. This message is accompanied by message numbers IRR68008I and IRR68009I.

System Action: Utility processing continues with recovery procedure.

User Response: If the problem recurs after following the user response for the indicated message numbers, record all information provided by all the messages and contact your IBM support center.

IRR68011I The utility has successfully completed.

Explanation: IRRRID00 has successfully finished processing. The decimal return code is zero.

IRR68012I The utility has not successfully completed.

Explanation: IRRRID00 found one or more errors during processing.

User Response: Review the messages produced by both IRRRID00 and the system. Take the actions appropriate to correct the problem.

IRR68013I The failing record number *record_number* is "*record_text*."

Explanation: If IRRRID00 has abended while processing a specific record, the first 60 bytes of the record are shown as *record_text*. *record_number* is the relative record number of the record. This message is accompanied by message numbers IRR68008I, IRR68009I, and IRR68010I.

IRR68014I *function_name* has completed with a return code of *return_code*.

Explanation: A function has returned a non-zero return code. *function_name* is the identifier of the function. If *function_name* is "SORT", then a call to the SORT product has returned a non-zero hexadecimal return code. If *function_name* is "ESTAE ESTABLISHMENT", then the establishment of the ESTAE recovery routine failed. *return_code* is the hexadecimal return code.

System Action: Utility processing stops with a decimal return code of 16.

User Response: Review the messages produced by the sort utility and take the actions indicated by those messages.

IRR68015I Record number *record_number* in INDD was not produced by IRRDBU00.

Explanation: IRRRID00 requires that valid IRRDBU00 output be used as input to INDD. IRRRID00 has determined that the record *record_number* was not generated by IRRDBU00.

System Action: Utility processing stops with a decimal return code of 16.

User Response: Be sure that INDD was allocated to a data set created by IRRDBU00 and that the data set's DCB characteristics are valid IRRDBU00 data set characteristics, specifically, that the record format is variable blocked (VB).

IRR68016I IRRRID00 was forced to truncate *count* records.

Explanation: The commands created by IRRRID00 are limited to 255 character lines. *count* is the number of commands that were created in which IRRRID00 could not fit the profile name or member data into a 255 character line. A question mark (?) in the left hand column shows the command lines that have been truncated.

System Action: The utility truncates the line on the right, sets the utility decimal return code to 4, and continues processing.

User Response: Review the truncated command that IRRRID00 created and process it manually if required.

IRR68017I The ID *id* in the *class* profile *profile_name* is not correct.

Explanation: IRRRID00 has found a profile containing an ID value that was not of the correct class. For example, the NOTIFY field must contain a user ID. If it contained a group ID, this message would be issued. *ID* is the ID value that is in error. *class* is the class of this profile. *profile_name* is the name of the profile, truncated to 20 characters.

System Action: The utility places commands to correct the error (for example, deleting all references of the 'ID') into the OUTDD data set. Message IRR68018I follows this message. The utility continues processing.

User Response: Review and verify all references of the ID should be deleted, and if necessary, edit the commands created by IRRRID00.

IRR68018I The record number is *record_number*. The ID value should be a *class* profile.

Explanation: This message identifies the profile that contains an incorrect ID value. *record_number* is the relative number of the input record that contained the ID value. *class* is the class that the ID value should be. Message IRR68017I precedes this message.

IRR68019I • IRR71004E

System Action: The utility continues processing.

User Response: Review and, if necessary, edit the commands created by IRRRID00.

IRR68019I IRRRID00 has searched *s_count* records and processed *l_count* records. (hh:mm:ss)

Explanation: Periodically, IRRRID00 indicates the number of IRRDBU00 records that it has processed. *hh:mm:ss* is the time that the message was issued. *s_count* is the number of records that have been searched for residual IDs. *l_count* is the number of records that have been processed, from which commands are generated.

This message is issued only if you have not supplied any user IDs or group IDs to search for.

You can look at the messages produced by the SORT program to see the total number of records that are being processed.

System Action: The utility continues processing.

User Response: None. This message is for informational purposes only.

IRR68020I IRRRID00 has processed *l_count* records. (hh:mm:ss)

Explanation: Periodically, IRRRID00 indicates the number of IRRDBU00 records that it has processed.

hh:mm:ss is the time that the message was issued. *l_count* is the number of records that have been processed, from which commands are generated.

This message is issued only if you have not supplied any user IDs or group IDs to search for.

You can look at the messages produced by the SORT program to see the total number of records that are being processed.

System Action: The utility continues processing.

User Response: None. This message is for informational purposes only.

IRR68021I IRRRID00 requires more storage to process all the IDs. *nnnn* Kbytes of additional storage is required.

Explanation: IRRRID00 requires memory for the storage of all the user IDs and group IDs. IRRRID00 was unable to acquire sufficient storage to process all of your IDs. *nnnn* is the number of kilobytes of additional storage required.

User Response: Allocate more storage by increasing the REGION under which the utility executes by at least *nnnn* kilobytes.

System Action: Utility processing stops, with a decimal return code 16.

REXX RACVAR messages

IRR71001E No arguments were specified for the function.

Explanation: A variable name was not specified for the RACVAR function. A variable name is required in the form RACVAR(*variable-name*).

System Action: EXEC processing stops.

User Response: Correct the RACVAR function and specify a variable name.

IRR71002E This system variable *xxx* is not supported for RACVAR processing.

Explanation: The variable name specified for the RACVAR function is not valid.

System Action: EXEC processing stops.

User Response: Correct the RACVAR function and specify a valid variable name in the form RACVAR(*variable-name*).

IRR71003E Multiple arguments are not allowed for the RACVAR function.

Explanation: The RACVAR function was specified with multiple arguments. Only one variable name is allowed for the RACVAR function.

System Action: EXEC processing stops.

User Response: Correct the RACVAR function and specify one variable name in the form RACVAR(*variable-name*).

IRR71004E No security information is available for the RACVAR function.

System Action: EXEC processing stops.

Explanation: No ACEE was available from which the information could be extracted.

User Response: Log off and log on again. Reenter the request that caused this message. If this message is issued again, report the message (and the request you were making) to your system programmer.

RACF subsystem messages

**IRRA001I UNABLE TO OBTAIN STORAGE FOR
 subsystem SUBSYSTEM ON
 INITIALIZATION.**

Explanation: The subsystem has not been successfully initialized due to the failure of GETMAIN to obtain storage for the main subsystem control block.

System Action: The initialization for the subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Make sure that sufficient storage is available in the common storage area (CSA) for this control block. For information on CSA storage estimates, refer to *z/OS Security Server RACF System Programmer's Guide*.

Destination: Descriptor code is 6. Routing code is 2.

**IRRA002I subsystem SUBSYSTEM HAS NOT
 BEEN INITIALIZED.**

Explanation: The indicated subsystem has not been successfully initialized. One or more previous messages have been issued providing specific information.

System Action: The initialization for the subsystem stops.

Operator Response: Report this message to your system programmer.

System Programmer Response: Refer to the previous messages for more specific information.

Destination: Descriptor code is 6. Routing code is 2.

**IRRA003I subsystem SUBSYSTEM
 INITIALIZATION TERMINATED IN
 ABEND HANDLING.**

Explanation: The initialization task for the indicated subsystem has detected an abend while attempting to process a previous abend.

System Action: The task stops.

Operator Response: Report this message to your system programmer.

System Programmer Response: Determine the cause for the abend from previous error messages.

Destination: Descriptor code is 6. Routing code is 2.

**IRRA004I UNABLE TO LOCATE MODULE *module*
 IN PROGRAM PROPERTIES TABLE.**

Explanation: Initialization for the RACF subsystem was not able to find the indicated module defined in the program properties table.

System Action: The address space discontinues initialization.

Operator Response: See the System Programmer Response or contact your system programmer.

System Programmer Response: Make sure that the proper PPT entry is defined in Parmlib member SCHEDxx for the RACF subsystem mainline module.

**IRRA007I The command prefix *prefix* could not
 be registered for subsystem *subsystem*.
 Return code X'*retcode*' and reason
 code X'*rsncode*' specify the MVS CPF
 error.**

Explanation: The attempt to register command prefix *prefix* for subsystem *subsystem* failed with MVS command prefix facility (CPF) return code *retcode* and reason code *rsncode*.

System Action: The RACF subsystem is not available.

System Programmer Response: Refer to the MVS documentation on the CPF to determine the problem. Use the MVS DISPLAY OPDATA command, if necessary, to see if the command prefix is already registered.

Destination: Descriptor code is 4. Routing code is 2.

**IRRA008I The system is in XCF-local mode.
 Scope of the command prefix *prefix* for
 subsystem *subsystem* has defaulted to
 SYSTEM.**

Explanation: The requested sysplex scope defaulted to SYSTEM scope for the indicated subsystem because the system is running in XCF-local mode.

System Action: Initialization continues.

Operator Response: Notify the system programmer.

System Programmer Response: Correct the scope in the IEFSSNxx parmlib member parameter. If needed, IPL the system for the change to take effect.

Destination: Descriptor code is 4. Routing code is 2.

**IRRA009I Error encountered while processing
 the IEFSSNxx for the subsystem
 subsystem. CPF system-wide default
 will be used.**

Explanation: An incorrect value was encountered while processing the IEFSSNxx parmlib member for the subsystem *subsystem* parameter. CPF system-wide default is used.

System Action: Initialization continues. Subsequent subsystem commands have only a system-wide scope.

System Programmer Response: Correct the scope in the IEFSSNxx parmlib member parameter. If needed, IPL the system for the change to take effect.

Destination: Descriptor code is 4. Routing code is 2.

IRRA010I **Error encountered while processing the IEFSSNxx for the subsystem *subsystem*. Prefix will be truncated to eight characters.**

Explanation: An incorrect value was encountered while processing the IEFSSNxx parmlib member for the subsystem *subsystem* parameter. The prefix is truncated.

System Action: Initialization continues.

System Programmer Response: Correct the length of the IEFSSNxx parmlib member parameter. If needed, IPL the system for the change to take effect.

Destination: Descriptor code is 4. Routing code is 2.

IRRA011I **OUTPUT FROM *command-name*:**

Explanation: A RACF command was issued from the operator console. After this message is issued, the output from command *command-name* is displayed at the operator console.

Destination: Descriptor codes are 5 and 6. Routing code is 2.

IRRA080I ***subsystem* SUBSYSTEM INITIALIZATION ENCOUNTERED AN ERROR. ABEND CODE IS *cde-rc*.**

Explanation: The initialization task for the indicated subsystem has encountered an abnormal condition.

System Action: The task attempts to restart.

Operator Response: Contact your system programmer.

System Programmer Response: The system abend dump contains more detailed information regarding the problem encountered by the indicated subsystem initialization task.

IRRB000I ***subsystem* SUBSYSTEM NOT DEFINED TO SYSTEM, TERMINATING.**

Explanation: The subsystem name could not be located in the SSCT control blocks. The *subsystem* being searched for is indicated in the message.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Add the subsystem name to the appropriate MVS subsystem name table (see IEFSSNxx PARMLIB member).

Destination: Descriptor code is 6. Routing code is 2.

IRRB001I ***subsystem* SUBSYSTEM *ver.rel.mod* IS ACTIVE.**

Explanation: Subsystem *subsystem* is active. The version is *ver*, the release is *rel*, and the modification is *mod*.

System Action: None.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRB002I **INITIALIZATION COMPLETE FOR *subsystem* SUBSYSTEM**

Explanation: All of the initialization for the indicated subsystem environment has been completed.

System Action: The subsystem is ready to accept operator commands.

Operator Response: None.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRB003I ***subsystem* SUBSYSTEM NOT RUNNING AS A STARTED TASK.**

Explanation: The indicated subsystem was not started as a started task.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Restart the indicated subsystem as a started task. (This message could reflect an error in the ICHRIN03 started task table).

Destination: Descriptor code is 6. Routing code is 2.

IRRB004I **RACF SUBSYSTEM ALREADY ACTIVE.**

Explanation: An attempt was made to start another RACF subsystem while the current subsystem is still active. RACF does not allow more than one RACF subsystem to be active.

System Action: The command is terminated.

System Programmer Response: If no RACF subsystem is active, verify that the ENQ resource (major name SYSZRACF and minor name RACF) was not propagated from some other system.

Destination: Descriptor code is 6. Routing code is 2.

IRRB005I *subsystem* **SUBSYSTEM TERMINATION IS COMPLETE.**

Explanation: The indicated subsystem stops.

System Action: None.

Operator Response: Check accompanying message and take appropriate action.

Destination: Descriptor code is 6. Routing code is 2.

IRRB006I *subsystem* **SUBSYSTEM MAIN TASK ABENDED IN ABEND HANDLING.**

Explanation: While attempting to handle an abend the indicated subsystem task encountered another abend in abend-handling code.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Examine console log and system abend dumps for more detailed information. Determine the cause of the first abend and restart.

Destination: Descriptor code is 6. Routing code is 2.

IRRB007I **RESTART LIMIT *nn* EXCEEDED FOR TASK *taskname* IN *subsystem* SUBSYSTEM.**

Explanation: The task indicated by *taskname* has exceeded the limit *nn* for automatic restarts by the main task in the indicated subsystem.

System Action: Task *taskname* is not restarted.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Examine the console log for abend messages about the particular problem.

Destination: Descriptor code is 6. Routing code is 2.

IRRB008I *subsystem* **IS NOT OPERATING IN AN AUTHORIZED MODE.**

Explanation: The job step failed APF authorization.

System Action: The indicated subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Ensure that RACF subsystem modules are linked into an authorized library with AC(1).

Destination: Descriptor code is 6. Routing code is 2.

IRRB009I *subsystem* **SUBSYSTEM INTERFACE MODULE *xxxxxxx* COULD NOT BE FOUND.**

Explanation: The named subsystem could not locate the indicated subsystem interface module.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Ensure that the module indicated in the message is in LNKSTxx library.

Destination: Descriptor code is 6. Routing code is 2.

IRRB010I *subsystem* **SUBSYSTEM INITIALIZATION FAILED TO BUILD THE SUBSYSTEM VECTOR TABLE.**

Explanation: The subsystem interface module found that the number of address vectors contained in the address vector table module exceeded the available number of entries in the SSVT table.

System Action: The indicated subsystem stops.

Operator Response: Report this message to your system programmer.

System Programmer Response: Make sure that the address vector table module is at the proper level with respect to the size of the SSVT table.

Destination: Descriptor code is 6. Routing code is 2.

IRRB011I **UNABLE TO OBTAIN STORAGE FOR *subsystem* SUBSYSTEM**

Explanation: Initialization for subsystem *subsystem* could not obtain storage for subsystem control blocks in common storage.

System Action: The subsystem is not initialized.

Operator Response: Report the text of this message to your system programmer.

System Programmer Response: Determine the cause of the storage shortage, fix the problem, and restart the address space.

Note: Storage for subsystem control blocks is in CSA (not ECSA).

Destination: Descriptor codes is 6. Routing code is 2.

IRRB012I *subsystem* **INITIALIZATION HAS RETURNED AN UNKNOWN RETURN CODE *rc*.**

Explanation: Initialization for the indicated subsystem returned an unexpected return code.

System Action: The subsystem stops.

IRRB013I • IRRB019I

Operator Response: Report this message to your system programmer.

System Programmer Response: Report the exact text of this message to your IBM support along with a list of recently applied RACF maintenance.

Destination: Descriptor code is 6. Routing code is 2.

IRRB013I RACF IS NOT ACTIVE. *subsystem* SUBSYSTEM TERMINATED.

Explanation: The subsystem does not operate unless RACF is active.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Determine cause of RACF failure, reactive RACF, and restart the subsystem.

Destination: Descriptor code is 6. Routing code is 2.

IRRB014I *subsystem* SUBSYSTEM IS NOT OPERATING UNDER A RACF-DEFINED USERID.

Explanation: The subsystem does not have a valid user ID in the started procedures table (ICHRIN03) or in the RACF database.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Enter a valid RACF user ID in the started procedures table for the subsystem named in the message. For more information about this table, see *z/OS Security Server RACF System Programmer's Guide*.

Destination: Descriptor code is 6. Routing code is 2.

IRRB015I *taskname* TASK IN *subsystem* SUBSYSTEM HAS TERMINATED ABNORMALLY.

Explanation: During the shutdown process, the subtask *taskname* in the subsystem *subsystem* would not voluntarily shut down. The main task has waited a sufficient interval for the subtask to end, without success. The subtask is forcefully ended.

System Action: Subtask *taskname* ends abnormally. The subsystem continues the shutdown process.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Examine any system dumps obtained.

Destination: Descriptor code is 6. Routing code is 2.

IRRB016I *subsystem* SUBSYSTEM NOT SUPPORTED IN THIS ENVIRONMENT

Explanation: The subsystem *subsystem* is only supported on MVS systems at or above the 3.1.3 level. The subsystem has detected that the current operating environment does not meet this requirement. You can also get this message when RACF initialization fails to complete successfully.

System Action: Subsystem *subsystem* stops.

User Response: Report the exact text of this message to your system programmer.

System Programmer Response: Do not attempt to exercise this function on an MVS system below the indicated level.

Destination: Descriptor code is 6. Routing code is 2.

IRRB017I *taskname* TASK HAS ABENDED WITH A CODE OF *cde-rc* IN *subsystem* SUBSYSTEM.

Explanation: The main task has detected an MVS system completion code in subtask *taskname* as indicated by completion code *cde*, reason code *rc* in subsystem *subsystem*.

System Action: The current command is ignored. The subsystem attempts to restart the subtask.

Operator Response: None.

System Programmer Response: Determine the cause of the subtask abend.

Destination: Descriptor code is 6. Routing code is 2.

IRRB019I MESSAGE *message-number* COULD NOT BE ISSUED DUE TO A FAILURE DURING MESSAGE PROCESSING.

Explanation: An error occurred while attempting to issue message *message-number*. The message is undefined or an I/O error occurred.

System Action: Message processing for the requested message ends.

User Response: Contact the system programmer. If the message exists in *z/OS Security Server RACF Messages and Codes*, the most likely cause of this message is that an incomplete RACF service update was applied.

System Programmer Response: Verify service application for accuracy. If there is no problem with service application and this message persists, this indicates an I/O problem while issuing the message and requires further investigation.

Destination: Descriptor code is 6. Routing code is 2.

IRRB020I *task* **TASK HAS BEEN RESTARTED.**

Explanation: The subsystem has restarted the task for which a prior RESTART command was issued.

Operator Response: None.

IRRB021I **UNABLE TO LOAD SERVICE ROUTINE**
(*routine*). *subsystem* **SUBSYSTEM**
TERMINATED.

Explanation: Service routine *routine* is needed for proper execution of the indicated subsystem but could not be loaded during initialization.

System Action: The indicated subsystem stops.

Operator Response: Notify the system programmer of the error.

System Programmer Response: Ensure that service routine *routine* resides in the LNKST concatenation.

Destination: Descriptor code is 6. Routing code is 2.

IRRB022I **SUB=MSTR WAS NOT SPECIFIED ON**
THE START *subsystem-name*
COMMAND. COMMAND IS IGNORED.

Explanation: A START command without the SUB=MSTR parameter was issued to start *subsystem-name* subsystem. *subsystem-name* is a RACF subsystem that can only be started under the master subsystem.

System Action: The command is ignored. The specified RACF subsystem is not started.

Operator Response: To start a RACF subsystem, issue the START command with the SUB=MSTR parameter.

Destination: Descriptor code is 6. Routing code is 2.

IRRB031I **TSO STACK HAS RETURNED A**
RETURN CODE OF *xx* **IN** *subsystem*
SUBSYSTEM.

Explanation: The STACK macro returned a nonzero return code (*xx*) when an attempt was made to direct the input and output of a TSO command to specified files.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Using the *xx* value, determine the cause of the condition and correct it. For an explanation of the return code, see *z/OS TSO/E Programming Services*.

Destination: Descriptor code is 6. Routing code is 2.

IRRB032I *subsystem* **SUBSYSTEM UNABLE TO**
OBTAIN STORAGE FOR *xxxx*
CONTROL BLOCK.

Explanation: The storage requested by the GETMAIN for the *xxxx* control block was not available. The possible values for *xxxx* are PSCB, UPT, ECT and LWA.

System Action: Subsystem *subsystem* stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Ensure that a sufficient region size is specified on the subsystem JCL.

Problem Determination: See message IRRB038I for additional problem determination information.

Destination: Descriptor code is 6. Routing code is 2.

IRRB033I *subsystem* **SUBSYSTEM UNABLE TO**
ALLOCATE FILE *subsystem* **FOR TSO**
STACK USAGE.

Explanation: The dynamic allocation request for the input or output file to be used by the TSO STACK macro has failed. See message IRRB034I for more dynamic-allocation error information.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Ensure that the subsystem JCL permits dynamic allocation.

Destination: Descriptor code is 6. Routing code is 2.

IRRB034I **DYNAMIC ALLOCATION**
INFORMATION: S99INFO IS *xxxx*,
S99ERROR IS *yyyy*.

Explanation: Dynamic allocation failed for either an input or an output file for use with the TSO STACK macro. This message follows the IRRB033I message.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Restart the subsystem after taking the action indicated for the dynamic-allocation error condition.

Destination: Descriptor code is 6. Routing code is 2.

IRRB036I **OPERATOR COMMAND PREFIX**
(*subsystem-name*) **MAY NOT BE AS**
SPECIFIED IN IEFSSNxx FOR
subsystem-name **SUBSYSTEM.**

Explanation: The operator restarted the subsystem after one of the following occurred:

IRRB037E • IRRB041I

- The initialization module failed to initialize the subsystem. Message IRRB037E is also issued.
- An operator was told to restart the subsystem manually with PARM=INITIAL.
- CPF registration was requested but failed. Message IRRB041I is also issued.

The subsystem name is used as the command prefix.

System Action: RACF does not attempt to register the default command prefix (the subsystem name) with CPF as a result of this message. Subsystem initialization continues.

Operator Response: Report the exact text of this message (IRRB037E) and message IRRB041I or IRRB040I, if either was issued, to your system programmer.

System Programmer Response: If message IRRB041I was issued, refer to the message explanation for that message.

If message IRRB040I was issued, refer to the return and reason codes given in that message for additional information in determining the problem.

Fix the problem before the next IPL. Use the default command prefix (the subsystem name) for this IPL.

Destination: Descriptor code is 6. Routing code is 2.

IRRB037E RESTART LIMIT OF *nn* EXCEEDED, subsystem SUBSYSTEM TERMINATED.

Explanation: The indicated subsystem mainline task has exceeded the limit for automatic restarts.

System Action: The subsystem is not restarted.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Examine the console log and any relevant system dumps to determine cause of abends. Attempt manual restart of the system using PARM=INITIAL option.

Destination: Descriptor code is 11. Routing code is (1,9).

IRRB038I STORAGE REQUESTED IS *yyyy*; SUBPOOL IS *zzz*.

Explanation: This message is issued after IRRB032I and indicates the storage and subpool requested by the GETMAIN.

System Action: See message IRRB032I.

Operator Response: See message IRRB032I.

System Programmer Response: See message IRRB032I.

Destination: Descriptor code is 6. Routing code is 2.

IRRB039E ABEND ENCOUNTERED BEFORE subsystem SUBSYSTEM INITIALIZED.

Explanation: The indicated subsystem encountered an initialization failure and further processing for the subsystem stops.

System Action: The subsystem stops.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Examine the console log and the system abend dump for more information.

Destination: Descriptor code is 11. Routing code is (1,9).

IRRB040I RESTART BEING ATTEMPTED FOR *ttttttt* TASK.

Explanation: The task indicated by *ttttttt* has encountered an abend and is attempting to restart.

System Action: The subsystem attempts to restart by detaching and reattaching the *ttttttt* task.

Operator Response: Report the exact text of the message to your system programmer.

System Programmer Response: Examine the console log for previously issued RACF messages or dumps and determine the cause of the problem.

Destination: Descriptor code is 6. Routing code is 2.

IRRB041I *ttttttt* TASK HAS ENDED WITH A CODE OF *return-code* IN *subsystem* SUBSYSTEM.

Explanation: The task indicated by *ttttttt* detached with an incomplete return code as indicated in *return-code*, which is displayed in hexadecimal format. The task may have ended because of an abend or the unexpected failure of a system service.

System Action: RACF restarts the task and the RACF subsystem continues normal operation. Tasks automatically restart up to five times between address space initializations or between uses of the RESTART command for a particular task.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Refer to the console log or dumps, if any, to determine the problem.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB042I TSO ENVIRONMENT SERVICE
REASON CODE IS** *reason-code*.

Explanation: IKJTSEV returned the code *reason-code* following its invocation during subsystem initialization.

Operator Response: Report the text of this and related messages to the system programmer.

System Programmer Response: See related message IRRB043I and appropriate TSO documentation for problem determination.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB043I TSO ENVIRONMENT SERVICE DETAIL
CODE IS** *code*.

Explanation: IKJTSEV returned the code *code* following its invocation during subsystem initialization.

Operator Response: Report the text of this and related messages to the system programmer.

System Programmer Response: See the appropriate TSO documentation for problem determination.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB048I *subsystem-name* SUBSYSTEM USING
PREVIOUS JCL PARM SPECIFICATION
OF:** *yy*.

Explanation: The *subsystem-name* subsystem is initializing using the value *yy* saved from a prior initialization. The RACF parameter library data set is as specified in the current JCL for the indicated subsystem.

System Action: The *subsystem-name* subsystem attempts to initialize.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB049I *subsystem-name* SUBSYSTEM IS NOT
ABLE TO ESTABLISH TSO
ENVIRONMENT, STATUS FOLLOWS:**

Explanation: The TSO service IKJTSEV failed. It was invoked by the indicated subsystem and is necessary for proper execution of that subsystem.

System Action: The indicated subsystem ends.

Operator Response: Report the text of this and related messages to the system programmer.

System Programmer Response: See related messages IRRB042I, IRRB043I, IRRB050I for a determination of the problem.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB050I TSO ENVIRONMENT SERVICE RETURN
CODE IS** *return-code*.

Explanation: IKJTSEV returned the code *return-code* following its invocation during subsystem initialization.

Operator Response: Report the text of this and related messages to the system programmer.

System Programmer Response: See related message IRRB042I and appropriate TSO documentation for problem determination.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB064I *subsystem-name* JCL PARM
SPECIFICATION IS:** *yyyyyyyyyy*.

Explanation: The *subsystem-name* is initializing using the member *yyyyyyyyyy* specified. If *yyyyyyyyyy* specifies a valid parameter library member, the RACF parameter library data set (as specified in the current JCL of *subsystem-name*) is searched for the appropriate member whose configuration statements are to be processed.

System Action: The *subsystem-name* subsystem attempts to initialize.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB065I *subsystem-name* PARAMETER LIBRARY
MEMBER SUFFIX STRING CONTAINS
INCORRECT CHARACTER(*y*). SUFFIX
IS IGNORED.**

Explanation: A correct member suffix can contain only alphanumeric characters, and *y* is not alphanumeric.

System Action: The indicated subsystem attempts to initialize without processing RACF parameter library configuration statements.

Operator Response: The configuration statements that were to be processed by reference to a RACF parameter library member can be processed after subsystem initialization via the SET INCLUDE command.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB066I *subsystem-name* PARAMETER LIBRARY
MEMBER SUFFIX STRING IS NULL. 00
IS ASSUMED.**

Explanation: In the absence of a named suffix, 00 is used to form the name of the RACF parameter library member whose configuration statements are to be processed (IRROPT00).

System Action: The indicated subsystem attempts to find the IRROPT00 member of the RACF parameter

IRRB067I • IRRB073I

library and process its configuration statements.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRB067I *subsystem-name* **PARAMETER LIBRARY MEMBER SUFFIX STRING IS LONGER THAN 2 CHARACTERS. SUFFIX IS IGNORED.**

Explanation: The given suffix has a length that exceeds the allowed maximum.

System Action: The indicated subsystem attempts to initialize without processing RACF parameter library configuration statements.

Operator Response: The configuration statements that were to be processed by reference to a RACF parameter library member can be processed after subsystem initialization via the SET INCLUDE command.

Destination: Descriptor code is 6. Routing code is 2.

IRRB068I *subsystem-name* **SUBSYSTEM WAS UNABLE TO BUILD ITS SCREEN TABLE. INITIALIZATION CONTINUES.**

Explanation: An error during initialization of the *subsystem-name* subsystem prevents the successful delivery of output from directed RACF commands via TSO XMIT. The delivery of such output to user data sets is unaffected.

System Action: Subsystem initialization continues.

Operator Response: Report the text of this message to the system programmer.

System Programmer Response: Report the occurrence of the error to the IBM support center.

Destination: Descriptor code is 6. Routing code is 2.

IRRB069I *subsystem-name* **SUBSYSTEM STARTING SHUTDOWN PROCESSING.**

Explanation: The indicated subsystem has started shutdown processing in response to an operator STOP command.

System Action: The indicated subsystem is in the process of ending all subsystem-related functions and will stop.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRB070I *subsystem-name* **SUBSYSTEM UNABLE TO PERFORM RESTART.**

Explanation: The indicated subsystem was not able to process the RESTART command at this time.

System Action: RACF continues processing.

Operator Response: Retry the command at a later time. If this message continues, issue the RESTART CONNECTION command. If the RESTART CONNECTION command also fails, you must stop the affected RACF subsystem address space by issuing the STOP *subsystem-name* command and then issue the MVS START command to start the started procedure for the RACF address space.

Destination: Descriptor code is 6. Routing code is 2.

IRRB071I *node-name* **UNDEFINED. COMMAND NOT PROCESSED.**

Explanation: The indicated node name is not defined to RRSF.

System Action: RACF continues processing.

Operator Response: Reenter the command and make sure you type the correct node name.

Destination: Descriptor code is 6. Routing code is 2.

IRRB072I **EXTRANEIOUS CHARACTERS WERE FOUND AFTER STOP COMMAND FOR *subsystem-name* SUBSYSTEM. COMMAND NOT PROCESSED.**

Explanation: Extraneous characters were found in the STOP command issued for subsystem *subsystem-name*.

System Action: RACF continues processing.

Operator Response: If you want to bring down the RACF subsystem address space, reenter the RACF STOP command without any trailing text.

Destination: Descriptor code is 6.

IRRB073I **EXTRANEIOUS TEXT DETECTED IN RESTART COMMAND. COMMAND *function* PROCESSED. EXTRANEIOUS CHARACTERS WERE IGNORED.**

Explanation: Extraneous characters were found after function *function* on the RESTART command. RESTART is valid only for one function at a time. All information specified after the first function is ignored.

System Action: RACF ignores the extraneous characters and continues processing.

Operator Response: None.

Destination: Descriptor code is 6.

**IRRB074I INCORRECT KEYWORD
 ENCOUNTERED FOR RESTART.**

Explanation: A RESTART command was issued with an incorrect keyword specified.

System Action: The command is not processed but RACF continues processing.

Operator Response: Reissue the RESTART command using valid keywords.

Destination: Descriptor code is 6.

**IRRB075I NOT AUTHORIZED TO ISSUE THE
 command COMMAND.**

Explanation: The user attempting to issue the indicated command is not authorized to the proper profile in the OPERCMDS resource class.

System Action: The indicated command ends without further processing.

Operator Response: Notify the security administrator.

RACF Security Administrator Response: Define the correct profile to the OPERCMDS class.

Destination: Descriptor code is 6.

**IRRB076I RESTART CONNECTION NODE IN
 PROGRESS FOR LOCAL NODE
 node-name.**

Explanation: A restart connection for the indicated node was initiated.

System Action: RACF restarts the connection for local node services.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB077I SYSNAME SHOULD NOT BE
 SPECIFIED WHEN NODE(*) IS
 SPECIFIED ON THE RESTART
 COMMAND.**

Explanation: When specifying NODE(*) to restart connections to all nodes, a specific SYSNAME cannot be specified.

System Action: The RESTART command is ignored.

Operator Response: Correct and reissue the command. You can enter NODE(*) SYSNAME(*) or NODE(*node-name*) SYSNAME(*system-name*).

Destination: Descriptor code is 6.

**IRRB078I RRSF NODE *node-name* IS A
 SINGLE-SYSTEM NODE AND THE
 SYSNAME PARAMETER SHOULD NOT
 BE SPECIFIED.**

Explanation: RRSF node *node-name* is a single-system node and the SYSNAME keyword cannot be specified.

System Action: The RESTART command is ignored.

Operator Response: Correct and reissue the command.

Destination: Descriptor code is 6.

**IRRB079I RRSF NODE *node-name* IS A
 MULTISYSTEM NODE AND THE
 SYSNAME PARAMETER SHOULD BE
 SPECIFIED.**

Explanation: When NODE *node-name* is specified, the SYSNAME() keyword is mandatory in order to RESTART the connection to a specific system in the multisystem node.

System Action: The RESTART command is ignored.

Operator Response: To restart connections to all systems within a multisystem node, specify NODE(*node-name*) SYSNAME(*) on the RESTART command. To restart the connection to a specific system within a multisystem node, specify NODENAME(*node-name*) SYSNAME(*system-name*).

Destination: Descriptor code is 6.

**IRRB080I RRSF NODE(S) WITH CONNECTION
 STATUS OF {DEFINED | DORMANT}
 WILL NOT BE RESTARTED.**

Explanation: RRSF nodes in the DEFINED or DORMANT state do not have an existing conversation and does not restart.

System Action: RESTART CONNECTION to nodes in the DEFINED or DORMANT state are ignored. The command continues processing nodes in other states.

Operator Response: None.

Destination: Descriptor code is 6.

**IRRB081I INCORRECT RRSF NODE NAME
 ENTERED ON THE RESTART
 COMMAND.**

Explanation: An RRSF node name with an incorrect length was entered on the RESTART CONNECTION command. The node name must be 1 to 8 characters.

System Action: The RESTART command is not processed.

Operator Response: Reissue the RESTART command using a valid node name.

IRRB082I • IRRC007I

Destination: Descriptor code is 6.

IRRB082I INCORRECT SYSNAME ENTERED ON THE RESTART COMMAND.

Explanation: A system name with an incorrect length was entered on the RESTART CONNECTION command. The system name must be 1 to 8 characters.

System Action: The RESTART command is not processed.

Operator Response: Reissue the RESTART command using a valid system name.

Destination: Descriptor code is 6.

IRRC001I MAXIMUM NUMBER *nn* OF COMMAND TASKS EXCEEDED FOR *subsystem* SUBSYSTEM. LAST COMMAND IGNORED.

Explanation: The RACF subsystem allows *nn* simultaneously active command-processing modules and ignores all requests in excess of this number. This message is not issued on systems running RACF version 2 release 2 or the z/OS Security Server.

System Action: The RACF subsystem continues operation.

Operator Response: Reenter the command.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRC002I *subsystem* SUBSYSTEM COMMAND SCAN ERROR. CODE IS *cde-rc*.

Explanation: The TSO command scan service failed with return code *cde*, reason code *rc*.

System Action: RACF subsystem *subsystem* stops.

Operator Response: Report the complete text of this message to your system programmer.

System Programmer Response: Determine the cause of the command scan error.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRC003I COMMAND *command-name* IS NOT VALID.

Explanation: Command *command-name* is not syntactically correct.

System Action: The RACF subsystem ignores the request and continues operation.

Operator Response: Reenter the command with the correct syntax.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRC004I COMMAND *cccccccc* IS NOT SUPPORTED.

Explanation: The RACF subsystem does not support the entered command.

System Action: The RACF subsystem ignores the request and continues operation.

Operator Response: None.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRC005I UNABLE TO LOAD MODULE *module-name* FOR *subsystem* SUBSYSTEM. COMMAND NOT EXECUTED.

Explanation: Command module *module-name* could not be loaded.

System Action: The RACF subsystem ignores the request and continues operation.

Operator Response: None.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRC006I *subsystem* SUBSYSTEM COMMAND HANDLING TASK TERMINATED IN ABEND PROCESSING.

Explanation: The indicated subsystem command-handling task experienced an abend during the handling of a previously encountered abend.

System Action: The indicated subsystem detaches the abending command-processing task and attempts to reattach the task. If the task continues to abend, the task permanently remains detached and the address space continues operation.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Examine abend dumps and fix the problem before the next IPL.

Destination: Descriptor code is 6. Routing code is 2.

IRRC007I ROUTE OF RACF *command* COMMAND TO MULTIPLE SYSTEMS IS NOT SUPPORTED. REISSUE THE COMMAND TO A SINGLE SYSTEM ONLY.

Explanation: The RACF command was prefixed with the MVS ROUTE command, directing the command to multiple members of a sysplex. This is allowed only for the RACF DISPLAY, SIGNOFF, and RVARY commands

and only when no RVARY keyword other than LIST is specified, either explicitly or by default. The RACF command must be reissued to a single member only.

System Action: The RACF subsystem ignores the request and continues operation.

Operator Response: Reissue the command to a single member.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRC010I UNABLE TO ESTABLISH RACF ENVIRONMENT FOR COMMAND
command.

Explanation: The command running in the RACF subsystem address space did not run because the appropriate security environment was not established.

System Action: The resources associated with running the failed command are released and the subsystem proceeds with the next command request, if any.

Operator Response: Check the RACROUTE return and reason codes from the following IRRC011I, IRRC012I, or IRRC021I messages for corrective action.

Destination: Descriptor code is 6.

IRRC011I RACROUTE RETURN
CODE=*SAF-return-code*, **RACF RETURN**
CODE=*return-code*, **RACF REASON**
CODE=*reason-code*. **USER ID IS** *userid*.

Explanation: A RACROUTE REQUEST=VERIFY was used to create the security environment required to run one of the following in the RACF subsystem address space:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

The RACROUTE failed.

System Action: The resources associated with running the failed command are released and the subsystem proceeds with the next command request, if any.

Operator Response: Check the RACROUTE REQUEST=VERIFY return and reason codes in *z/OS Security Server RACROUTE Macro Reference* for an explanation of the codes.

Note: The reason and return codes in this message are displayed in decimal format. The codes presented in *z/OS Security Server RACROUTE*

Macro Reference are shown in hexadecimal format.

The RACROUTE return code is also called the SAF return code.

Destination: Descriptor code is 6.

IRRC012I TARGET USER ID *node.userid* **DOES NOT EXIST.**

Explanation: The RACF subsystem address space attempted to issue one of the following on behalf of the named user, but the user is not defined to RACF:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

This message is issued in conjunction with IRRC010I.

System Action: Command processing fails to complete.

User Response: If the command was a directed command from another node, the command issuer should correct the user name in the AT keyword. If the command was an automatically directed command from another node, contact your RACF security administrator.

RACF Security Administrator Response: Ensure that matching user IDs exist on nodes participating in automatic command direction processing.

Destination: Descriptor code is 6. Routing code is 2.

IRRC013I Password synchronized successfully
for *source-userid* **at** *source-node* **and**
target-userid **at** *target-node*.

Explanation: A password synchronization request that was originated by the source user ID has been completed for the target user ID. This is an informational message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

IRRC014I Password synchronization request
ignored for *userid* **at** *node-name*. **An**
approved PEER PWSYNC association
was not found.

Explanation: An attempt has been made to process a password synchronization request. However, an approved PEER PWSYNC association was not found in the target user's RACF user profile. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User Response: Verify the RACF association between

IRRC015I • IRRC019I

the source and target user IDs or contact your RACF security administrator.

IRRC015I **Unable to communicate with the RACF subsystem. IEFSSREQ return code is**
return-code.

Explanation: RACF attempted to process a password change request for a user. The password change has been made on this system's RACF database. However, if associations exist with another user on this or a remotely connected system, the passwords will not be synchronized. Report this message to your system programmer. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The system continues processing.

System Programmer Response: The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

Code	Explanation
4	The subsystem does not support this function.
8	The subsystem exists, but is not active.
12	The subsystem is not defined in the IEFSSNxx parmlib member.
16	The function has not completed. This is a disastrous error.
20	The SSOB or SSIB have lengths or formats that are not valid.
24	The SSI has not been initialized.

A return code of 4, 16, 20 or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See *z/OS Security Server RACF System Programmer's Guide* for configuration considerations for the RACF subsystem.

IRRC016I **User ID *userid* is not defined to use a password.**

Explanation: RACF password synchronization attempted to process a password change request for a user. The user ID in the message is not required to enter a password, but is identified via an OIDCARD. RACF password synchronization is not applicable to the user ID in this message. This is an informational message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User Response: If you do not want to see this message every time the associated user ID changes his

or her password, either disable password synchronization for the user who initiated the password change, or have the security administrator alter this user ID profile to require a password using the ALTUSER command.

IRRC017I **Unable to verify PWSYNC association with userid *userid*.**

Explanation: RACF attempted to verify the RACF association with the user ID shown in the message. The verification attempt was not successful. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User Response: Use the RACLINK LIST command to list the associations for the user ID in the message to determine the nature of the failure, or report this message to your administrator.

IRRC018I **Unable to set password date. Return code is**
return-code. Reason code is
reason-code.

Explanation: RACF attempted to propagate an update to the PASSDATE field of the RACF user profile identified in the user's RRSFLIST data set, but was unable to complete the update. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The PASSDATE field of the user profile was not updated. The system continues processing.

User Response: Examine the return and reason codes to determine the nature of the problem. The return and reason codes displayed in this message have been returned from the RACF database manager. For a description of the RACF manager return codes, refer to "RACF Manager Return Codes" on page 307.

IRRC019I **Password synchronization request could not be performed. Return code is**
return-code. Reason code is
*reason-code. User *userid* not processed.*

Explanation: A password synchronization request for the user ID could not be processed. RACF has encountered an error. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User Response: Report this message to your RACF system administrator. The password of the user ID has not been changed.

System Programmer Response: Examine the return and reason codes to determine the nature of the problem. The return and reason codes displayed in this message have been returned from the RACF database

manager. For a description of the RACF manager return codes, refer to “RACF Manager Return Codes” on page 307.

IRRC020I Passdate was set for *userid* at *node-name*.

Explanation: RACF has successfully updated **only** the password change date in the specified user ID profile. This is an informational message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User Response: None required.

IRRC021I ACCESS HAS BEEN REVOKED FOR USER ID *userid*.

Explanation: The RACF subsystem address space attempted to issue one of the following on behalf of the indicated user ID, but that user ID's access has been revoked:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

This message is issued with IRRC010I. It is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: Verify that the user ID specified is correct. If it is, contact the RACF security administrator.

RACF Security Administrator Response: A command has been directed either manually or automatically to a user ID whose access has been revoked. Take whatever action the site RACF security policy requires for requests made on behalf of revoked users.

IRRC022I RACF REMOTE SHARING CONNECTION TO NODE *node-name* [SYSNAME *system-name*] HAS CHANGED FROM {OPERATIVE ACTIVE | OPERATIVE PENDING CONNECTION | OPERATIVE PENDING VERIFICATION} TO OPERATIVE ERROR. FAILURE OCCURRED WHEN APPC VERB *verb* WAS ISSUED. RETURN CODE = {APPC RETURN-CODE | NOT RESPONDING}

Explanation: The local RACF RRSF node is unable to communicate with the indicated node. The state of the connection has been changed to operative error. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The RACF subsystem address space saves the request that was issued and when the problem has been corrected, RACF sends the request to the indicated node.

Operator Response: Refer to the APPC/MVS documentation for information on the APPC verb and return code to determine the cause of the communication failure. Correct the problem and restart the connection using the TARGET command.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC023I RACF REMOTE SHARING SERVER COULD NOT BE REGISTERED TO APPC/MVS. FAILURE OCCURRED WHEN APPC VERB *verb* WAS ISSUED. RETURN CODE = {APPC RETURN-CODE} REASON CODE = {APPC REASONCODE}

Explanation: The local RACF remote sharing server could not be registered to APPC/MVS using the information provided in the RACF parameter library or entered in the TARGET command. This message is seen if APPC is made unavailable on a NODE that has previously been registered as an APPC server. Also, this message appears if the LU which is being used to register RRSF as an APPC/MVS server was defined as SCHED instead of NOSCHED.

System Action: The RACF subsystem address space cannot send or receive any remote sharing requests. The requests are saved and when the problem has been corrected, RACF sends the requests.

Operator Response: Refer to the APPC/MVS documentation to determine why RACF was unable to register as an APPC/MVS server. Also, refer to the APPC/MVS documentation to determine if the APPC reason code indicated in this message is a meaningful field for the the APPC return code indicated in this message. Verify that the LU which is being used to register RRSF as an APPC/MVS server has been defined with the NOSCHED option in member APPCPMxx in SYS1.PARMLIB. Correct the problems and issue the TARGET command to make the local node operative.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC024I RACF REMOTE SHARING CONNECTION TO NODE *node-name* [SYSNAME *system-name*] DID NOT COMPLETE SUCCESSFULLY. FAILURE OCCURRED WHEN APPC VERB *verb* WAS ISSUED. RETURN CODE = {APPC RETURN-CODE}

Explanation: The local RACF remote sharing connection to a remote RACF RRSF node was unable

IRRC025I • IRRC029I

to successfully execute an APPC/MVS verb. Here are some typical causes:

- VTAM or APPC is not active on the local or remote node.
- VTAM or APPC has been unable to connect to the server on the remote node.
- A TARGET command has not been issued to make the remote node OPERATIVE.
- The appropriate RACF security definitions have not been provided.

If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The RACF subsystem address space cannot send or receive any remote sharing requests to the remote node.

Operator Response: Check the status of the connection by using the TARGET command on both the local and remote node. Issue the appropriate TARGET commands to place the connection into the state desired. If the two nodes are in the desired state, refer to the APPC/MVS documentation to determine why RACF was unable to successfully execute the APPC/MVS verb. Correct the problems and issue the TARGET command to make the local node operative.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC025I RACF REMOTE SHARING SERVER COULD NOT BE REGISTERED TO APPC/MVS IN THE ALLOTTED TIME INTERVAL. FAILURE OCCURRED WHEN APPC VERB *verb* WAS ISSUED.

Explanation: The RACF remote sharing facility (RRSF) was unable to establish itself as an APPC/MVS server. The specific APPC/MVS verb did not complete within thirty minutes.

System Action: RRSF is unable to make any new connections to other remote RRSF nodes. Work for the remote nodes is being queued until they can be activated.

Operator Response: Refer to the documentation on isolating the cause of the communication failure. Correct the problems and restart the connection using the TARGET command.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC026I RACF REMOTE SHARING REQUEST TO NODE *node-name* [SYSNAME *system-name*] COULD NOT BE COMPLETED IN THE ALLOTTED TIME INTERVAL. FAILURE OCCURRED WHEN THE APPC VERB *verb* WAS ISSUED.

Explanation: The local RACF RRSF node is unable to complete a request to the indicated node. If SYSNAME information is present in this message, the node *node-name* is a multisystem node. This message goes to the SYSLOG and is accompanied by other messages.

System Action: The RACF subsystem address space saves the request that was issued and when the connection has been made, RACF sends the request to the indicated node.

IRRC028I RACF REMOTE SHARING SERVER HAS DE-REGISTERED FROM APPC/MVS.

Explanation: The RACF address space has registered as an APPC/MVS server when the appropriate TARGET command was issued. This registration is being ended by either a request (TARGET, RESTART CONNECTION, or STOP) sent by a person or by the RACF remote sharing facility (RRSF) because of a failure within the subsystem.

System Action: The RACF subsystem stops processing APPC/MVS allocate requests from other RRSF nodes.

Operator Response: When it is appropriate for RRSF to accept APPC/MVS allocate requests from another node, issue the appropriate TARGET commands.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC029I RACF REMOTE SHARING MODULE *module-name* HAS EXPERIENCED A FAILURE WITH THE VSAM FILE *data-set-name*. IRRSSQ00 REQUEST = *request*, IRRSSQ00 RETURN CODE = *module-return-code*, GRS RETURN CODE = *GRS-return-code*.

Explanation: RACF remote sharing experienced a failure when it attempted to checkpoint a request to a specific VSAM file. The IRRSSQ00 REQUEST is either:

- R - read
- X - read_next
- I - insert
- E - erase

The IRRSSQ00 RETURN CODE indicates either a logic or a GRS failure:

Code	Explanation
------	-------------

- 1 ACB pointer or DSNAM not set in the node definition block
- 2 ENQ
- 3 Unknown request type
- D DEQ

The GRS RETURN CODE definitions can be found in *z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN* or *z/OS MVS Programming: Authorized Assembler Services Reference ENF-IXG*. If the IRRSSQ00 RETURN CODE is either 1 or 3, the GRS RETURN CODE is set to zero and should be ignored.

System Action: The RACF subsystem address space is not able to send or receive remote sharing requests for the specified node.

Operator Response: Determine why RACF remote sharing experienced the failure when checkpointing information to the VSAM file. Check for other instances of either this message, or message IRRC030I, and LOGRECs. A 'd grs,res=(syszrac3,*)' may be issued from the MVS master console for major name SYSZRAC3 ENQ information. A 'd grs,c' issued from the MVS master console may be used to display all outstanding resource contention. If the IRRSSQ00 RETURN CODE is either 1 or 3, report this problem to the IBM support center. Correct the problems. Once the problem has been resolved, start the node using the TARGET command (for example, TARGET NODE(x) OPERATIVE ...).

Destination: Descriptor code is 6. Routing code is 2.

IRRC030I **RACF REMOTE SHARING MODULE**
module-name **HAS EXPERIENCED A**
FAILURE WITH THE VSAM FILE
data-set-name. **IRRSSQ00 REQUEST =**
request, **IRRSSQ00 RC =**
module-return-code, **VSAM RC =**
vsam-return-code, **SHOWCB RC =**
showcb-return-code, **VSAM REASON**
CODE = *vsam-reason-code*

Explanation: RACF remote sharing experienced a failure when it attempted to checkpoint a request to a specific VSAM file. The IRRSSQ00 REQUEST is either:

- R - read
- X - read_next
- I - insert
- E - erase

The IRRSSQ00 RETURN CODE indicates a VSAM failure:

- | Code | Explanation |
|------|----------------|
| 4 | MODCB RPL ACB |
| 5 | MODCB RPL AREA |

- 6 MODCB RPL RECLEEN
- 7 MODCB RPL ARG
- 8 MODCB RPL OPTCD=NUP
- 9 GET
- A PUT
- B ERASE
- C ENDREQ
- E OPEN

The VSAM RETURN CODE, SHOWCB RETURN CODE, and VSAM REASON CODE definitions may be found in *z/OS DFSMS Macro Instructions for Data Sets*. If the SHOWCB RETURN CODE is non-zero, the value for the VSAM REASON CODE should be ignored.

System Action: The RACF subsystem address space is not able to send or receive remote sharing requests for the specified node.

Operator Response: Determine why RACF remote sharing experienced the failure when checkpointing information to the VSAM file. Typical causes of this problem are the VSAM file is full or the disk containing the VSAM file is experiencing I/O errors. Check for other instances of either this message, or message IRRC029I, and LOGRECs. Correct the problems. Once the problem has been resolved, start the node using the TARGET command (for example, TARGET NODE(x) OPERATIVE ...).

Destination: Descriptor code is 6. Routing code is 2.

IRRC031I *subsystem-name* **SUBSYSTEM DATA**
SET *data-set-name* **IS FULL.**

Explanation: The indicated workspace data set on the indicated subsystem is full.

System Action: Processing for this directed or RACLINK command stops.

Operator Response: Contact your system programmer or data management expert.

System Programmer Response: Allocate a larger VSAM data set. See *z/OS Security Server RACF System Programmer's Guide* for information on the procedure to follow.

Destination: Descriptor code is 6. Routing code is 2.

IRRC032I **RACF REMOTE SHARING**
CONNECTION TO NODE *node-name*
[SYSNAME *system-name* **] HAS**
CHANGED FROM {DORMANT LOCAL |
DORMANT BY MUTUAL REQUEST } TO
DORMANT ERROR.

Explanation: The local RACF remote sharing facility (RRSF) node is unable to checkpoint RRSF requests for

IRRC033I • IRRC036I

the indicated node. A VSAM file used to checkpoint requests is not functional. If SYSNAME information is present in this message, node *node-name* is a multisystem node.

System Action: The RACF subsystem stops all processing for this node until the problem with the VSAM file is resolved.

Operator Response: Refer to the VSAM documentation on isolating the cause of the VSAM failure. RACF message IRRC029I or IRRC030I contains the return and reason codes describing the VSAM failure. Correct the problems and redefine the VSAM files using the TARGET command.

Destination: Descriptor code is 6. Routing code is 2.

**IRRC033I RACF REMOTE SHARING
CONNECTION TO NODE *node-name*
[SYSNAME *system-name*] HAS
CHANGED FROM {OPERATIVE ACTIVE
| OPERATIVE PENDING CONNECTION |
OPERATIVE PENDING VERIFICATION |
DORMANT REMOTE } TO OPERATIVE
ERROR.**

Explanation: The local RACF remote sharing facility (RRSF) node is unable to send an RRSF request to the indicated node. The VSAM file used to checkpoint requests is the most likely cause of the problem. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The RACF subsystem stops all processing for this node until the problem is resolved.

Operator Response: Review the system log for accompanying messages. If the problem was caused by the VSAM file, refer to the VSAM documentation on isolating the cause of the VSAM failure. RACF message IRRC030I or IRRC031I contains the VSAM return and reason codes describing the VSAM failure. Correct the problems and redefine the VSAM files using the TARGET command.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

**IRRC034I RACF IS UNABLE TO ESTABLISH A
TSO I/O ENVIRONMENT FOR
COMMAND *command*. TSO STACK HAS
RETURNED A RETURN CODE OF
return-code.**

Explanation: The command running in the RACF subsystem address space did not run because the appropriate TSO I/O environment could not be established.

System Action: The resources associated with the failed command are released and the subsystem proceeds with the next command request, if any.

Operator Response: Report the exact text of this

message to your system programmer.

System Programmer Response: Use the indicated TSO STACK return code to determine the cause of the condition and correct it. For an explanation of the return code, see *z/OS TSO/E Programming Services*.

Destination: Descriptor code is 6. Routing code is 2.

**IRRC035I You have not been authorized for
password synchronization.**

Explanation: Your RACF user profile contains approved peer user ID associations with password synchronization with other user IDs. However, your RACF security administrator has not authorized your password changes to be synchronized by RACF. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: Your RACF password has been changed only in your RACF user profile.

User Response: Report this message to your RACF security administrator. The users allowed to use password synchronization are determined by the installation.

RACF Security Administrator: If appropriate, give the user READ access to the PWSYNC profile in the RRSFDATA class.

Problem Determination: The ability to synchronize passwords is protected via RACF profiles in the RRSFDATA class. Ensure that the RRSFDATA class is active, profiles are up to date (that is, RACLIST REFRESH if you have the class RACLISTed), and that you have the proper authority granted to the profile covering the PWSYNC entity. See *z/OS Security Server RACF Security Administrator's Guide* for more details.

**IRRC036I This password synchronization request
was originated by *userid* at *node-name*.**

Explanation: RACF has processed a password synchronization request that was originated on your behalf by the user ID specified in the message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User Response: No action required. This is an informational message.

IRRC037I **AN AUTOMATIC PASSWORD DIRECTION REQUEST COULD NOT BE PERFORMED. RACROUTE RETURN CODE IS** *saf-return-code*, **RACF RETURN CODE IS** *return-code*, **RACF REASON CODE IS** *reason-code*. **USER** *userid* **NOT PROCESSED.**

Explanation: A password synchronization request could not be performed. RACF encountered an error on a RACROUTE REQUEST=VERIFY statement. This message is appended to your RRSFLIST data set.

User Response: Report this message to your RACF system programmer.

System Programmer Response: Check the RACROUTE REQUEST=VERIFY return and reason codes in *z/OS Security Server RACROUTE Macro Reference* for an explanation of the codes. The RACROUTE return is also called the SAF return code.

IRRC038I **A request to process Kerberos key information for user** *user* **failed. Processing continues.**

Explanation: An error occurred while attempting to generate a Kerberos key for a user password change.

System Action: All processing except for the key update is completed.

User Response: Report this message to the system programmer and provide the exact text of the message.

System Programmer Response: Use the RLIST command to list the KERBDFLT profile definition of the local Kerberos realm in the REALM class and verify that the local realm name (KERBNAME) is defined. Use the LISTUSER command to list the KERB segment information for this user and verify that this information may be accessed. Correct any problems and ask the user to do another password change.

IRRC080I *subsystem-name* **SUBSYSTEM COMMAND HANDLING TASK ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*.

Explanation: The command handler task was scheduling the running of a RACF command. This message appears when an abnormal event occurs. It is written to the SYSLOG.

System Action: The command handler attempts to retry the current work request.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of

ABEND, the subtask should resume processing any work in its input queue. Refer to “Actions to Recover from an RRSF Failure” in *z/OS Security Server RACF Diagnosis Guide* for a complete discussion.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: See *z/OS MVS System Codes* for an explanation of these codes.

Destination: Descriptor code is 6. Routing code is 2.

IRRC081I *subsystem-name* **SUBSYSTEM COMMAND HANDLING TASK ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*. **COMMAND HANDLING TASK ENDING.**

Explanation: The COMMAND handler task was scheduling the running of a RACF command, a password change, or an application update in the RACF subsystem. This message appears when an abnormal event occurs.

System Action: When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of ABEND, the subtask should resume processing any work in its input queue. Refer to “Actions to Recover from an RRSF Failure” in *z/OS Security Server RACF Diagnosis Guide* for a complete discussion.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: See *z/OS MVS System Codes* for an explanation of these codes. The task that started the COMMAND handling task attempts to restart the task. Verify that message IRRB020I was issued showing that the task was successfully restarted.

Destination: Descriptor code is 6. Routing code is 2.

IRRC110I **Unable to establish RACF environment for application update request.**

Explanation: The application update did not run in the RACF subsystem address space because the appropriate security environment was not established.

System Action: The resources associated with running the failed update request are released and the subsystem proceeds with the next request, if any.

User Response: For corrective action, check the RACROUTE return and reason codes from the IRR011I, IRR012I, or IRR021I message that follows.

DISPLAY command messages

**IRRD000I DISPLAY ENCOUNTERED AN ERROR
WHILE USING TSO PARSE, PARSE
RETURN CODE WAS *nn***

Explanation: During the parse of the DISPLAY command image, the TSO parse facility returned a code that is documented in *z/OS TSO/E Programming Services* in the section discussing IKJPARS.

System Action: The DISPLAY command stops further processing and does not display any of the requested information.

Operator Response: Verify that the DISPLAY command was correctly entered with the desired keywords and associated operands. Reenter the command, and if the condition persists, notify your system programmer.

User Response: See operator response.

System Programmer Response: Examine the original DISPLAY command image for possible specification errors. Use the *nn* value to determine the specific cause of the TSO Parse condition.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRD001I UNIDENTIFIED TEXT OR KEYWORD
text IN DISPLAY COMMAND**

Explanation: The *text* character string was present in the DISPLAY command image and was not recognized as a valid keyword.

System Action: The DISPLAY command stops.

Operator Response: Examine the DISPLAY command image and correct the text indicated by the *text* string. Refer to for information on *z/OS Security Server RACF Command Language Reference* the DISPLAY command.

User Response: See operator response.

System Programmer Response: See operator response.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRD002I NOT AUTHORIZED TO ISSUE THE
DISPLAY COMMAND**

Explanation: The user attempting to issue the DISPLAY command is not authorized to the proper profile in the **OPERCMDS** resource class.

System Action: The DISPLAY command stops without further processing.

Operator Response: Notify either the security administrator or the system programmer.

User Response: See the operator response.

System Programmer Response: Either define the correct profile to the **OPERCMDS** class or notify the security administrator.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRD003I DISPLAY COMMAND TERMINATED IN
ABEND PROCESSING**

Explanation: During the recovery processing of an abend condition another abend was detected.

System Action: The DISPLAY command stops without further processing.

Operator Response: Notify either the system programmer or the security administrator. Note whether the DISPLAY command provided any previous messages (such as IRRD080I), and whether a system dump has been taken.

User Response: See the operator response.

System Programmer Response: Determine what keywords and operands are contained in the DISPLAY command. Examine the console log prior to this message for the presence of other messages that might provide further information. Also, examine the system dump data sets for the presence of a dump resulting from this condition.

Destination: Descriptor code is 1. Routing codes are 2 and 9.

IRRD004I RACF *v.rr.m* SUBSYSTEM

Explanation: This message is for information only and indicates the current version *v*, release *rr*, and modification level *m* of the installed RACF product. Depending on the operands, one of the following groups of message lines may be displayed. "LU" in these messages is the abbreviation for "logical unit".

When the APPL keyword is specified with no other keywords:

LU NAME LU NAME ... LU NAME *applname1*
applname2 ... *applname7*

When the POE keyword is specified without the USER, GROUP, or SECLABEL keywords:

REMOTE LU NAME(S) ASSOCIATED WITH ACTIVE
LOCAL LU NAME *applname* LU NAME LU NAME
... LU NAME *poename1 poename2* ... *poename7*

When USER, GROUP, or SECLABEL keywords are specified:

LOCAL LU *applname* FOR REMOTE LU *poename* HAS THE FOLLOWING USER(S): USER = *userid* GROUP = *group* SECLABEL = *seclabel*

When the POE keyword is specified and there are no matches for a particular APPL:

NO REMOTE LU NAMES MATCHING *poename* WERE FOUND FOR LOCAL LU *applname*

When the user-group-seclabel combination cannot be located:

NO USERS MEET THE SPECIFIED CRITERIA

System Action: The DISPLAY command continues processing any specified operands.

Destination: Descriptor codes are 5, 8, and 9. There are no routing codes for this message.

IRRD005I DISPLAY COMMAND UNABLE TO LOCATE APPL *APPL-name*

Explanation: The *APPL-name* specified in the APPL keyword could not be found in the table of current local LU (logical unit) names. This message is produced for explicit *APPL-name*.

System Action: The DISPLAY command stops without further processing.

Operator Response: Check that the *APPL-name* name entered in the APPL keyword is correct. Reenter the command with the proper value. If the problem persists notify the system programmer or the security administrator.

User Response: See the operator response.

System Programmer Response: If the *APPL-name* is known to exist in the table of current local LU-names, obtain diagnostic information such as a system dump containing the table of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRD006I DISPLAY COMMAND UNABLE TO LOCATE A MATCH FOR APPL *APPL-name*

Explanation: The APPL(*APPL-name*) specification was not matched by an entry in the table of local LU (logical unit) names. This message is produced when the *APPL-name* specification is of the form APPL(ABC*) or APPL(*).

System Action: The DISPLAY command stops without processing.

Operator Response: Check the *APPL-name* entered in the APPL keyword for correctness. Reenter the command with the proper value. If the problem persists

notify the system programmer or the security administrator.

User Response: See the Operator Response.

System Programmer Response: If the *APPL-name* is known to match at least one entry in the table of current local LU names, obtain diagnostic information such as a system dump containing the table of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRD007I DISPLAY COMMAND FOUND THAT THERE WERE NO LOCAL LUS CURRENTLY ACTIVE

Explanation: The DISPLAY command could not display any information because the table of local LU (logical unit) names was empty.

System Action: The DISPLAY command stops without further processing.

Operator Response: No specific response is required for this message unless it is known that the table should not be empty. In that case, notify the system programmer or the security administrator.

User Response: See the Operator Response.

System Programmer Response: If this message reflects a condition that should not be present, examine the console log to determine what operations have been performed on the table of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRD008I DISPLAY COMMAND UNABLE TO LOCATE USER INFORMATION FOR REMOTE LU NAME *poename*

Explanation: The DISPLAY command could not display any information because the list of signed-on users is empty.

System Action: The DISPLAY command stops without further processing.

Operator Response: No specific response is required for this message unless you know that the list should not be empty. In that case, if the list is empty, notify the system programmer or the security administrator.

User Response: See the Operator Response.

System Programmer Response: If this message reflects a condition that should not be present, examine the console log to determine what operations have been performed on the list of signed-on users.

Destination: Descriptor code is 2. There are no routing codes for this message.

**IRRD009I DISPLAY COMMAND FOUND THAT
THERE WERE NO USERS CURRENTLY
SIGNED ON**

Explanation: There are no users in the signed-on list or lists.

System Action: The DISPLAY command stops without further processing.

Operator Response: No response is required unless it is known that users are currently signed on. If users are signed on, verify that the DISPLAY command was correctly entered with the desired keywords and associated operands. If the command was entered correctly and users should be signed on, reenter the command and if the condition persists, notify your system programmer.

User Response: See the Operator Response.

System Programmer Response: Examine the original DISPLAY command image for possible specification errors. Examine the console logs to determine whether users have been signed off or some abnormal condition has occurred.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRD010I DISPLAY COMMAND ENCOUNTERED
AN INTERNAL ERROR. RETURN CODE
IS *return-code***

Explanation: The DISPLAY command encountered an internal error. The return code describes the type of error that was encountered.

Code Description

(Decimal)

- | | |
|----|----------------------------|
| 16 | Storage problem |
| 20 | Storage unavailable |
| 24 | Incorrect length exception |

- | | |
|----|------------------------------------|
| 28 | Inconsistency exception |
| 36 | Inconsistency exception |
| 40 | Operation rejected exception |
| 44 | Incorrect control data exception |
| 60 | Unexpected exception |
| 64 | Incorrect offset exception |
| 68 | Incorrect key definition exception |

Operator Response: Report this message along with the return code to your system programmer.

System Programmer Response: Report this message along with the return code to your IBM Support Center.

**IRRD080I DISPLAY COMMAND ENCOUNTERED
AN ERROR. ABEND CODE IS
*abend_code-reason_code***

Explanation: During the normal processing of the DISPLAY request an abnormal condition was detected. The *abend_code* and *reason_code* are displayed. Display the system dump data sets for an accompanying diagnostic dump.

System Action: The DISPLAY command stops processing.

Operator Response: Notify the system programmer.

User Response: Notify the system programmer.

System Programmer Response: Report this message ID and its contents to your IBM support center. For a description of the abend code and reason code, refer to Chapter 8, "RACF abend codes" on page 295. If the abend code and reason code displayed in the message do not appear in this manual, refer to the system codes manual for the MVS system at your installation.

RACDCERT command messages

**IRRD101I You are not authorized to issue the
RACDCERT command.**

Explanation: One of the following occurred:

- You are not defined to RACF with sufficient authority and cannot issue the RACDCERT command.
- RACF is not active.

System Action: RACDCERT command processing ends.

User Response: See your RACF security administrator. *z/OS Security Server RACF Command Language Reference* describes the authority required to issue the RACDCERT command.

**IRRD102I The user ID specified is not defined to
RACF.**

Explanation: The user ID specified on the ID keyword of the RACDCERT command could not be found on the RACF database.

System Action: RACDCERT command processing ends.

User Response: Be sure the user ID is specified correctly and that the user is defined to RACF. Issue the command again.

IRRD103I An error was encountered processing the specified input data set.

Explanation: RACDCERT encountered an error related to the data set containing the digital certificate or certificate request.

System Action: RACDCERT command processing ends.

User Response: Check that the correct data set name was specified for the ADD, CHECKCERT, GENCERT or MAP keywords. Check for additional error messages pertaining to the data set name.

IRRD104I The input data set does not contain a valid {certificate | certificate request}.

Explanation: RACDCERT encountered an error while attempting to analyze the digital certificate or certificate request contained in the data set.

System Action: RACDCERT command processing ends.

User Response: Check that the correct data set name was specified for the ADD, CHECKCERT, GENCERT or MAP keywords. If you specified ADD, CHECKCERT, or MAP, check that the correct data set name containing a certificate was specified. If you specified GENCERT, check that the correct data set name containing a certificate request was specified.

IRRD105I No certificate information was found for user *userid*.

Explanation: RACDCERT was unable to locate digital certificate information for the user ID indicated in the message.

System Action: RACDCERT command processing ends.

User Response: Check that the ID keyword was specified correctly.

IRRD106I Additional information is required to identify the certificate.

Explanation: RACDCERT located more than one digital certificate for this user. Sufficient information was not provided to uniquely identify the certificate to be acted on.

System Action: RACDCERT command processing ends.

User Response: Provide additional information on the DELETE or ALTER keyword to uniquely identify the digital certificate that you want deleted or altered. You might need one of the following to identify the certificate:

- SERIALNUMBER and ISSUERSDN
- LABEL

IRRD107I No matching certificate was found for this user.

Explanation: RACDCERT could not find a digital certificate for this user that matched the information provided.

System Action: RACDCERT command processing ends.

User Response: Check that the ID keyword was specified correctly. If you specified the SERIALNUMBER and ISSUERSDN keywords or the LABEL keyword, be sure they were specified correctly. Issue the RACDCERT command with the LIST keyword to examine the user's certificate information. The ISSUERSDN and LABEL must be specified in the same case as shown in the display, and must include any blank characters shown in the display.

IRRD108I The certificate does not meet RACF requirements and cannot be used.

Explanation: The data set contains a valid certificate, but it cannot be used by RACF for one of the following reasons:

- The combined length of the serial number and issuer's distinguished name is too long to create a DIGTCERT profile name. The combined length should not exceed the maximum length of 246 for a profile name.
- The certificate contains critical extensions that are not recognized by RACF.
- The certificate version is greater than 3.

System Action: RACDCERT command processing ends.

User Response: The digital certificate found in the data set cannot be used by RACF. If you have more than one certificate, be sure that the correct one was placed in the data set. Otherwise, you need to obtain a new certificate containing information that meets RACF requirements. If you cannot obtain another certificate, contact your system programmer.

System Programmer Response: Check that the certificate being used has been issued by the intended certifying authority. If necessary, report the problem to the IBM support center.

IRRD109I The certificate cannot be added. Profile *profile-name* is already defined.

Explanation: The DIGTCERT profile name derived from this certificate already exists on the RACF database.

System Action: RACDCERT command processing ends.

User Response: Use RACDCERT CHECKCERT to determine if the digital certificate is currently defined for

IRRD110I • IRRD116I

the correct user. If not, use RACDCERT DELETE to delete the certificate and issue the RACDCERT ADD command for the correct user.

IRRD110I **Unexpected RACROUTE REQUEST=***request-type* **error encountered during command processing. RACF RC =** *x'retcode***, RACF RSN =** *x'rsncode***.**

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System Action: RACDCERT command processing ends.

User Response: Report this message to the system programmer and provide the exact text of the command you issued.

System Programmer Response: Use the return code information in *z/OS Security Server RACROUTE Macro Reference* to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

IRRD111I **The certificate cannot be {added | altered}. The label** *label-name* **is already in use.**

Explanation: You attempted to add or alter a certificate and assign label *label-name* to it. This label is already in use for the user specified in the RACDCERT command.

System Action: RACDCERT command processing ends.

User Response: Choose a different label for the certificate and reissue the command.

IRRD112I **The {certificate | certificate request} that you are processing does not have a valid signature.**

Explanation: The certificate or certificate request that is contained in the data set specified with the ADD or GENCERT keyword does not have a valid signature or message authentication code (MAC). The certificate or certificate request might have been altered.

System Action: RACDCERT command processing ends.

User Response: If the certificate or certificate request has been altered, obtain an unaltered copy and add the certificate.

IRRD113I **The certificate that you are {adding | creating} error-description. The certificate is added with {TRUST | NOTRUST | HIGHTRUST} status.**

Explanation: You are using RACDCERT ADD or RACDCERT GENCERT to define a certificate to RACF. As a part of the definition process, RACF validates the date range on the certificate. This message might indicate that RACF has detected a potential date conflict. If *error-description* reads:

- "is self-signed," the certificate you are adding cannot be verified.
- "is expired," the last date for which the certificate is valid has passed and cannot be used to authenticate the user.
- "has an incorrect date range," the date range of the certificate being added is not within date range established by the certificate authority certificate.

System Action: RACDCERT adds the certificate.

User Response: Do one of the following:

- If you want to alter the trust status of the certificate, issue the RACDCERT ALTER command.
- If the date range is incorrect, get either a new certificate or a new certificate authority certificate from the issuer and add the certificate.

IRRD114I **Ring** *ring-name* **does not exist.**

Explanation: You attempted to reference the ring *ring-name*, which does not exist. To fit within a single line of message output, *ring-name* is truncated after approximately 200 characters.

System Action: RACDCERT command processing ends.

User Response: Select a ring name that exists for the user ID and reissue the RACDCERT command.

IRRD115I **User** *userid* **has no rings.**

Explanation: You issued a RACDCERT LISTRING command for a user who has no rings.

System Action: RACDCERT command processing ends.

User Response: None.

IRRD116I **Label** *label-name* **does not exist in ring** *ring-name* **for user** *userid*.

Explanation: You attempted to reference a certificate by the label *label-name*, which does not exist for user *userid* in *ring-name*. *ring-name* is truncated if its length plus the length of the static message text plus the length of *userid* plus the length of *label-name* is more than is able to fit within a single line of output.

System Action: RACDCERT command processing ends.

User Response: Select a label name that exists and reissue the RACDCERT command.

IRRD117I Unexpected ICSF *service-name* return code x'*return-code*' and reason code x'*reason-code*'. The request is not processed.

Explanation: RACDCERT received an unexpected return code *return-code* and reason code *reason-code* from ICSF service *service-name*.

System Action: The request is not processed.

User Response: See the ICSF documentation to determine how to resolve the unexpected return and reason codes from the ICSF service.

IRRD118I Unsupported encryption algorithm. {Certificate added with TRUST status. | Certificate added with NOTRUST status. | Certificate not created.}

Explanation: You are trying to add or generate a certificate from a certificate request. RACF cannot validate the signature because the algorithm that was used to generate the certificate's signature or the certificate request's signature is not supported by RACF.

System Action: If you are adding a certificate, the certificate is added with the trust status that you specified. If you didn't specify a trust status, the certificate is added with NOTRUST status. If you are generating a certificate, the certificate is not created.

User Response: Acquire a certificate or certificate request with a signature algorithm that is supported by RACF and reissue the RACDCERT ADD or RACDCERT GENCERT command. If the certificate was added, delete the old certificate.

IRRD119I Certificate Authority not defined to RACF. Certificate added with {TRUST | NOTRUST | HIGHTRUST} status.

Explanation: You are adding a certificate.

- If you are adding a self-signed certificate, the certificate content has not been verified.
- If you are adding a non-self-signed certificate, the certificate was signed by a certificate authority that you have not defined to RACF.

System Action: The certificate is added with the trust status indicated by the message.

- If you are adding a self-signed certificate and you didn't specify a trust status, the certificate is added with TRUST status.

- If you are adding a non-self-signed certificate and you did not specify a trust status, the certificate is added with NOTRUST status.
- The HIGHTRUST value will be used if specified, but will never be a default.

User Response: Review the certificate status and change it if necessary. If you want to change the trust status, you should use the RACDCERT ALTER command.

IRRD120I Incorrect use of {CERTAUTH | SITE}. A {Certificate Authority | Site Certificate} cannot own a key ring.

Explanation: You attempted to create a key ring for a site certificate or a certificate authority. This is not permitted. Only users may have key rings.

System Action: The command fails.

User Response: Correct the error and reissue the command.

IRRD121I A ring name and label name must be specified.

Explanation: You issued a RACDCERT CONNECT or RACDCERT REMOVE command without a ring name or a label name specified. These commands require you to specify both a ring name and a label name.

System Action: The command fails.

User Response: Correct the error and reissue the command.

IRRD122I Ring *ring-name* cannot be added. It already exists.

Explanation: A ring may be added only once. Ring *ring-name* already exists. *ring-name* is truncated if its length plus the length of the static message text is more than is able to fit within a single line of output. This means that *ring-name* is truncated after approximately 200 characters.

System Action: The command fails.

User Response: Choose a different name for the ring and reissue the command.

IRRD123I The certificate that you are processing is not encrypted. The certificate is not processed.

Explanation: You specified the PASSWORD keyword on a RACDCERT ADD or RACDCERT CHECKCERT request. The certificate contained in the data set you specified is not encrypted with a password.

System Action: RACDCERT does not process the certificate.

User Response: Check the data set to determine

IRRD124I • IRRD130I

whether to use the PASSWORD keyword and reissue the command correctly.

IRRD124I **The certificate that you are processing cannot be decrypted with the specified PASSWORD. The certificate is not processed.**

Explanation: The password you specified on a RACDCERT ADD or CHECKCERT request was not correct or the data set contains a certificate in a format that RACF cannot recognize. RACDCERT could not decrypt the certificate.

System Action: RACDCERT does not process the certificate.

User Response: Specify the correct password and reissue the command or acquire a certificate in a format that RACF can recognize.

IRRD125I **The SIZE value that was specified or defaulted is not acceptable. The request is not processed.**

Explanation: The key size is not acceptable. The maximum key size is determined by United States export restrictions or internal system limits. If the SIZE keyword is not specified, the key size defaults to 1024.

System Action: RACDCERT does not process the request.

User Response: Reissue the command with a SIZE value that is allowed.

IRRD126I **The {certificate | certificate request} contains either a key usage or basic constraint extension indicating that it may not be used as a Certificate Authority certificate. The certificate is not {added | generated}.**

Explanation: The certificate or certificate request extension contains information indicating that the certificate may not be used as a certificate authority certificate.

System Action: The command terminates.

Programmer Response: Acquire a correct certificate or certificate request and reissue the command.

IRRD127I **The data set contains a PKCS12 encrypted certificate. The PASSWORD keyword must be specified to process the certificate. The certificate is not processed.**

Explanation: The input data set is a PKCS12 certificate package, which requires that you specify a password for RACDCERT to process the certificate. You must specify the password that is associated with the

data set in the PASSWORD keyword.

System Action: RACDCERT does not add the certificate.

User Response: Issue the command with the PASSWORD keyword specified.

IRRD128I ***function-name* requires a certificate with an associated private key. The request is not processed.**

Explanation: The RACDCERT function *function-name*, which can be either GENCERT or GENREQ, requires a private key. GENCERT requires the private key that is associated with the certificate specified with the SIGNWITH keyword. GENREQ requires the private key that is associated with the certificate identified by the LABEL and the ID, SITE, or CERTAUTH keywords.

System Action: RACDCERT does not process the request.

User Response: Reissue the command with a valid signing certificate. You can use the RACDCERT LIST command to see if a certificate has a private key associated with it.

IRRD129I **Unexpected *service-name* return code *x'return-code*'. The request is not processed.**

Explanation: RACF calls non-RACF routines to perform specific operations. For example, RACF uses RSA's BSafe support to perform public key operations. *service-name* returns an unexpected hexadecimal return code, *return-code*. The valid values for *service-name* are BSafe and CEEPIPI.

System Action: RACDCERT does not process the request.

User Response: Report the problem to your system programmer. Services beginning with CEE are Language Environment services. Consult the documentation for those products to see additional diagnostic information. If *service-name* is not listed above, contact the RACF support center.

IRRD130I **The *keyword-name* keyword(s) must be specified. The request is not processed.**

Explanation: The command that you issued required you to specify keyword *keyword-name*. The required keyword was not specified. For example, the RACDCERT EXPORT and RACDCERT GENREQ functions require a data set name (using the DSN keyword) and a label name (using the LABEL keyword). If either of these keywords is omitted, this message is issued.

The following are additional explanations for the mapping functions:

- Neither IDNFILTER nor SDNFILTER was specified with MAP.
- MULTIID was specified for MAP without criteria.
- CRITERIA or NEWCRITERIA was specified with ID (or defaulting to ID).

System Action: RACDCERT does not process the request.

User Response: Specify the required keyword and reissue the command.

IRRD131I The specified SUBJECTSDN exceeds the maximum allowed (*mmm* characters) by *nnn* characters. The request is not processed.

Explanation: The total length of the subject's distinguished name is limited to 229 characters for self-signed certificates and 255 characters for non-self-signed certificates.

System Action: RACDCERT does not process the request.

User Response: Reduce the total length of the distinguished name in the SUBJECTSDN keyword by at least *nnn* characters and reissue the command.

IRRD132I The certificate specified in the SIGNWITH keyword is not trusted. The certificate is added with NOTRUST status.

Explanation: You signed a certificate with a certificate that is marked as NOTRUST. Your certificate is added with NOTRUST status.

System Action: RACDCERT adds the certificate with NOTRUST status.

User Response: If you want to create a trusted certificate, either reissue the RACDCERT GENCERT command or issue the RACDCERT ALTER command to make your certificate trusted.

IRRD133I The NOTBEFORE value must be earlier than the NOTAFTER value. The certificate is not created.

Explanation: You attempted to create a certificate with a NOTBEFORE date that was later than the NOTAFTER date. This is not allowed.

System Action: RACDCERT stops processing the request. The certificate is not created.

User Response: Correct the NOTBEFORE and NOTAFTER dates and reissue the RACDCERT GENCERT command.

IRRD134I An error was encountered processing the specified output data set.

Explanation: RACDCERT encountered an error related to the data set containing the output of the RACDCERT command.

System Action: RACDCERT command processing stops.

User Response: Check to be sure you entered the correct data set name. Check for additional errors pertaining to the data set name.

IRRD135I ICSF is not operational. The request is not processed.

Explanation: Either you are attempting to generate or add a certificate to the RACF database and have indicated that you wish to use ICSF for key management, or you are attempting to generate a certificate or certificate request where the private key required to sign the information is an ICSF key. ICSF is not available.

System Action: The command is not processed.

User Response: If ICSF is not required, reissue the command without requesting ICSF. If ICSF is required, report the error to your system programmer. Reissue the command after the problem has been corrected. For more information see *z/OS Security Server RACF Command Language Reference*.

System Programmer Response: Ensure that ICSF is configured for PKA support and operational. For more information see *z/OS z/OS ICSF System Programmer's Guide*.

IRRD136I MULTIID cannot be used for the function specified.

Explanation: You attempted a certificate related or key ring related function for the user ID MULTIID. This user ID is associated with filtering based on additional criteria, and can only be used for the mapping functions: MAP, ALTMAP, DELMAP and LISTMAP.

System Action: RACDCERT command processing ends.

User Response: Correct the error and reissue the command.

IRRD137I Incorrect use of [CERTAUTH | SITE]. A [Certificate Authority | Site Certificate] cannot be used for a mapping function.

Explanation: You attempted to associate a mapping profile with the user ID associated with certificate authority certificates or site certificates. This is not permitted. Only users or MULTIID can be associated with a mapping profile.

IRRD138I • IRRD145I

System Action: RACDCERT command processing ends.

User Response: Correct the error and reissue the command.

IRRD138I The Label *label-name* is already in use.

Explanation: You attempted to associate a user ID with a mapping profile, and assign *label-name* to that association, or you attempted to change the label of an existing mapping profile to *label-name*. The label is already in use for the user specified in the RACDCERT command.

System Action: RACDCERT command processing ends.

User Response: Chose a different label and reissue the command.

IRRD139I This filter already exists. It cannot be added.

Explanation: You specified values for the IDNFILTER and SDNFILTER keywords that would create a filter that already exists in a mapping profile in the DIGTNMAP class. All filters must be unique.

System Action: RACDCERT command processing ends.

User Response: Chose a different filter value, or delete the existing mapping, and reissue the command.

IRRD140I The filter value does not begin with a valid prefix.

Explanation: You specified a value for the IDNFILTER or SDNFILTER keyword that does not begin with a valid prefix. The value must begin with an X.509 identifier such as C= or OU=.

System Action: RACDCERT command processing ends.

User Response: Specify a valid prefix for the filter value, and reissue the command.

IRRD141I The starting point specified for [IDNFILTER | SDNFILTER] is not found in the certificate.

Explanation: You specified a value for the IDNFILTER or SDNFILTER keyword that does not correspond to any value in the certificate contained in the input data set.

System Action: RACDCERT command processing ends.

User Response: Use the CHECKCERT keyword to display the certificate, and reissue the command with filter values that correctly correspond to the names in the certificate.

IRRD142I The starting point specified for [IDNFILTER | SDNFILTER] results in a filter that is too long.

Explanation: You specified a value for the IDNFILTER or SDNFILTER keyword to be used as the starting point for a filter based on a certificate you have supplied in a data set. The resulting filter would exceed 255 characters from the specified starting point to the end of the actual name in the certificate.

System Action: RACDCERT command processing ends.

User Response: Use the CHECKCERT keyword to display the certificate, and reissue the command with a starting point value that is 255 characters or less from the end of the issuer's or subject's name.

IRRD143I No mapping profile with label *label-name* exists for this user ID.

Explanation: You specified a label name that does not exist for this user.

System Action: RACDCERT command processing ends.

User Response: Use the LISTMAP keyword without specifying a label to determine the label names that exist for this user. If you are attempting to alter or delete a mapping, reissue the RACDCERT command with the correct label.

IRRD144I No mapping profiles are associated with [user *userid* | MULTIID].

Explanation: You issued a RACDCERT LISTMAP command for a user who is not associated with any mapping profiles in the DIGTNMAP class.

System Action: RACDCERT command processing ends.

User Response: None.

IRRD145I A label is required to identify the mapping to be [altered | deleted].

Explanation: You specified ALTMAP or DELMAP without specifying a label. This user has more than one mapping profile entry associated with it, and a label is required to identify which mapping to change or delete.

System Action: RACDCERT command processing ends.

User Response: Reissue the RACDCERT command with the LABEL keyword specified.

IRRD146I SDNFILTER cannot be specified with a partial issuer's name filter.

Explanation: You specified both SDNFILTER and IDNFILTER for the MAP function, with a certificate supplied in a data set. The value specified for IDNFILTER does not correspond to the beginning of the issuer's name in the certificate. This indicates that a partial issuer's name is to be used for the filter value. The SDNFILTER keyword cannot be used to specify a subject's name filter if IDNFILTER specifies a partial issuer's name.

System Action: RACDCERT command processing ends.

User Response: Reissue the RACDCERT command without the SDNFILTER keyword, or specify a value for the IDNFILTER keyword that will result in the full issuer's name being used in the filter.

IRRD147I EXPORT in PKCS12 format requires a certificate with an associated non-ICSF private key. The request is not processed.

Explanation: A PKCS#12 certificate package contains a certificate and private key. The certificate you are trying to export either has no associated private key or has a private key stored in ICSF. (ICSF private keys are not exportable.)

System Action: The command stops.

Programmer Response: Do one of the following:

- Choose a certificate that has a non-ICSF private key.
- Export in a CERT format that does not require a private key.

IRRD148I EXPORT in PKCS12 format requires an encryption password. The PASSWORD keyword must be specified. The request is not processed.

Explanation: The data portion of a PKCS#12 certificate package is encrypted using a user specified password. The password was not specified.

System Action: The command stops.

Programmer Response: Reenter the command specifying the PASSWORD keyword.

IRRD149I PKCS12 EXPORT package created with an incomplete certificate basing chain.

Explanation: RACF could not locate one of the signing certificates because either it is not installed as a CERTAUTH certificate or is expired. A PKCS#12 certificate package contains the end certificate being exported and any signing certificates needed to complete the basing chain (hierarchy) from end certificate to self-signed root certificate.

System Action: An incomplete PKCS#12 certificate package is created.

Programmer Response: If a complete PKCS#12 package is required, be sure that the appropriate nonexpired signing certificates are installed under CERTAUTH. Reenter the command.

IRRD150I Extra Certificate Authority Certificates ignored. Processing continues for the end-entity certificate only

Explanation: You are attempting to add a PKCS#7 certificate package to RACF. The package contains an end-entity certificate and one or more Certificate Authority (CERTAUTH) certificates. You are not authorized to add CERTAUTH certificates.

System Action: The command continues. However, the CERTAUTH certificates are not added.

User Response: If the CERTAUTH certificates are required, see your RACF security administrator. *z/OS Security Server RACF Command Language Reference* describes the authority required to issue the RACDCERT command.

IRRD151I PKCS7 package created with an incomplete certificate basing chain

Explanation: You are attempting to export a PKCS#7 certificate package from RACF. A PKCS#7 certificate package contains the end-entity certificate being exported and any Certificate Authority (CERTAUTH) certificates needed to complete the basing chain (hierarchy) from end-entity certificate to self-signed root certificate. RACF could not locate one of the CERTAUTH certificates needed for one of the following reasons:

1. It is not installed as a CERTAUTH certificate.
2. It is expired.
3. You are not authorized to export CERTAUTH certificates.

System Action: An incomplete PKCS#7 certificate package is created.

User Response: If a complete PKCS#7 package is required, be sure that the appropriate non-expired Certificate Authority certificates are installed under CERTAUTH. Also, see your RACF security administrator. The *z/OS Security Server RACF Command Language Reference* describes the authority required to issue the RACDCERT command. Reenter the command.

IRRD152I Root Certificate Authority not currently defined to RACF. Top CERTAUTH certificate added with the {TRUST | NOTRUST | HIGHTRUST} status

Explanation: You are attempting to add a PKCS#7 certificate package to RACF. The package contains a end-entity certificate and a chain of one or more Certificate Authority (CERTAUTH) certificates. The issuer of the top CA certificate (i.e., the root Certificate Authority) is not currently defined to RACF. If the top CA certificate is a self-signed certificate, the certificate content has been verified using the public key contained in the certificate itself. If the top CA certificate is a non-self-signed certificate, the certificate was signed by a certificate authority that you have not defined to RACF and thus cannot be verified.

System Action: The top CA certificate is added under CERTAUTH with the trust status displayed. See *z/OS Security Server RACF Command Language Reference* for information on how the trust status was determined. Processing continues for the remaining certificates in the package.

User Response: Review the certificate status and change it if necessary. If you want to change the trust status, you should use the RACDCERT ALTER command.

IRRD153I Inconsistency detected for one or more Certificate Authority certificates. Processing continues for the end-entity certificate

Explanation: You are attempting to add a PKCS#7 certificate package to RACF. The package contains a end-entity certificate and one or more Certificate Authority (CERTAUTH) certificates. While adding the CERTAUTH certificates, an inconsistency was detected for one or more of these certificates. The inconsistency is one of the following:

1. The certificate is expired.
2. The certificate has an incorrect date range relative to the issuing CA certificate. (The validity period is not completely contained with the validity period of the issuing CA certificate.)
3. The issuer of the certificate is missing from the PKCS#7 package and is not already installed under CERTAUTH.

4. The certificate has an unknown signature algorithm.

System Action: The CERTAUTH certificates are added. In most cases, the trust status set for these certificates will be NOTRUST. See *z/OS Security Server RACF Command Language Reference* information on how the trust status was determined. Processing continues for the end-entity certificate.

User Response: If the CERTAUTH certificates are required, check the certificates that were added under CERTAUTH to determine which ones have the inconsistency. Contact your certificate supplier to determine if replacement certificates are available. If so, adding them will replace the inconsistent ones. Otherwise, if you wish to use the certificates as is, you should change their status to TRUST. To change the trust status, you should use the RACDCERT ALTER command.

IRRD154I PCICC is not operational. The request is not processed

Explanation: You are attempting to generate a certificate and have indicated that you wish to use the PCI cryptographic coprocessor (PCICC) or you are attempting to generate a certificate or certificate request where the private key required to sign the information is a PCICC key. The PCI cryptographic coprocessor is either not present or not operating.

System Action: The command is not processed.

User Response: If the PCI cryptographic coprocessor is not required, you can attempt to reissue the command without specifying the PCICC keyword. If the PCI cryptographic coprocessor is required, report the error to your system programmer. Reissue the command after the problem has been corrected. For more information, see *z/OS Security Server RACF Command Language Reference*.

System Programmer Response: Ensure that ICSF and the PCI cryptographic coprocessor are configured and operational. For more information, see *z/OS ICSF System Programmer's Guide*.

R_PKIServ callable service messages

IRRD201I Subject name missing from certificate request.

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify an existing certificate request using the R_PKIServ callable service MODIFYREQS function

but did not provide a subject's name.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: Check that you have provided some name information for the request, for example common name or title, or contact your system programmer or web page administrator.

Application Programmer Response: Check that the application invoking the R_PKIServ callable service is providing name information. (At least one of CommonName, Title, OrgUnit, Org, Locality, StateProv, or Country.)

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, make sure the certificate template definition in the pkiserv.tmpl file either permits the user to enter name information or the name information is present in the <CONSTANT> section.

IRRD202I Hostid mapping information is too large.

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify a PKI Services certificate request using the R_PKIServ callable service MODIFYREQS function but provided more than 1024 characters worth of Hostid mapping information. The total which is compared against the 1024 character limit is calculated by the following formula:

Total=Sum of (length of each subject-id@host-name specification +1) -1

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User and Administrator Response: Check that the values you have provided for the Hostid mapping fields do not total more than 1024 characters.

IRRD203I Subject's name exceeds the maximum allowed (255 characters).

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify an existing certificate request using the R_PKIServ callable service MODIFYREQS function but provided a subject's name that is too long.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: Reduce the length of the name information for the request such as common name, title, etc. or contact your system programmer or web page administrator.

Application Programmer Response: Modify the application invoking the R_PKIServ callable service to provide less name information.

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, modify the certificate template definition in the pkiserv.tmpl file to provide less name information in the <CONSTANT> section.

IRRD204I "PublicKey" encoding is not valid.

Explanation: You attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions. The certificate request containing the public key to be certified does not have a valid format. It must be a base64 encoded PKCS#10 certificate request or one generated internally by your web browser.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: If you are requesting a server certificate, make sure that the request was generated in the proper format. If you are requesting a browser certificate, make sure you are using a supported web browser. For more information, see *z/OS Security Server PKI Services Guide and Reference*.

IRRD205I "PublicKey" encoding does not have a valid signature.

Explanation: You attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions. The certificate request containing the public key to be certified does not have a valid signature. The certificate request might have been altered.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: If the certificate has been altered, obtain an unaltered copy and retry the request.

IRRD206I "PublicKey" encoding contains an unsupported encryption algorithm.

Explanation: You attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions. The certificate request containing the public key to be certified was signed using an unsupported encryption algorithm.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: If you are requesting a server certificate, make sure that the request was generated using a supported algorithm. If you are requesting a browser certificate, make sure you are using a supported web browser. For more information, see *z/OS Security Server PKI Services Guide and Reference*.

IRRD207I Incorrect KeyUsage specified.

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify an existing certificate request using the R_PKIServ callable service MODIFYREQS function but provided an incorrect combination of KeyUsage values. If you are specifying the KeyUsage via

keywords or PKI Services web page dialogs, CERTSIGN may not be specified in combination with either HANDSHAKE or DATAENCRYPT. If you are specifying the KeyUsage via KeyUsage flags in a PKCS#10 certificate request, keyCertSign cannot be specified in combination with either keyEncipherment or dataEncipherment.

System Action: R_PKIServ processing ends. RACF prevents the request from completing.

User Response: Select a different KeyUsage, generate a new PKCS#10 certificate, if applicable, or contact your system programmer or web page administrator.

Application Programmer Response: Modify the application invoking the R_PKIServ callable service to provide different KeyUsage values.

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, modify the certificate template definition in the pkiserv.tmpl file to provide different KeyUsage values in the <CONSTANT> section.

SIGNOFF command messages

IRRE000I SIGNOFF ENCOUNTERED AN ERROR WHILE USING TSO PARSE, PARSE RETURN CODE WAS *nn*

Explanation: During the parse of the SIGNOFF command image, the TSO parse facility returned return code *nn*, which is documented in *z/OS TSO/E Programming Services*, in the section discussing IKJPARS.

System Action: The SIGNOFF command stops processing and does not display any of the requested information.

Operator Response: Verify that the SIGNOFF command entered was correctly entered with the desired keywords and associated operands. Reenter the command. If the condition persists, notify your system programmer.

User Response: See the Operator Response.

System Programmer Response: Examine the original SIGNOFF command image for possible specification errors. Use the *nn* value to determine the specific cause of the TSO Parse condition.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE001I UNIDENTIFIED TEXT OR KEYWORD *text* IN SIGNOFF COMMAND.

Explanation: The *text* character string was present in the SIGNOFF command image and was not recognized as a valid keyword.

System Action: The SIGNOFF command stops.

Operator Response: Examine the SIGNOFF command image and correct the text indicated by the *text* string. For information on the SIGNOFF command, see *z/OS Security Server RACF Command Language Reference*.

User Response: See the Operator Response.

System Programmer Response: See the Operator Response.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE002I NOT AUTHORIZED TO ISSUE THE SIGNOFF COMMAND

Explanation: The user attempting to issue the SIGNOFF command is not authorized to the proper profile in the OPERCMDS resource class.

System Action: The SIGNOFF command stops without further processing.

Operator Response: Notify either the security

administrator or the system programmer.

User Response: See the Operator Response.

System Programmer Response: Either define the correct profile to the OPERCMDS class or notify the security administrator.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE003I SIGNOFF COMMAND TERMINATED IN ABEND PROCESSING

Explanation: During the recovery processing of an abend condition another abend was detected.

System Action: The SIGNOFF command stops without further processing.

Operator Response: Notify either the system programmer or the security administrator. Note whether the SIGNOFF command has provided any previous messages and whether a system dump has been taken.

User Response: See the Operator Response.

System Programmer Response: Determine what keywords and operands are contained in the SIGNOFF command. Examine the console log prior to this message for the presence of other messages that might provide further information. Also, examine the system dump data sets for the presence of a dump resulting from this condition.

Destination: Descriptor code is 1. Routing codes are 2 and 9.

IRRE004I SYSTEM AUTHORIZATION FACILITY REQUEST ENDED WITH A RETURN CODE OF *code*

Explanation: The attempt to issue a SIGNOFF request ended with a return code of *code*. This *code* has been returned by the System Authorization Facility (SAF) router. For an explanation of the return code, see *z/OS Security Server RACROUTE Macro Reference*.

System Action: The SIGNOFF command stops without further processing. Message IRRE006I follows this message with information about the return and reason codes from the RACF SIGNOFF request.

Operator Response: Notify either the system programmer or the security administrator. Note whether the SIGNOFF command provided any previous messages and whether a system dump was taken.

User Response: See the Operator Response.

System Programmer Response: Determine what keywords and operands are contained in the SIGNOFF command. Examine the portion of console log recorded near the time of this message for the presence of other

IRRE005I • IRRE009I

messages that might provide further information. Also, examine the system dump data sets for the presence of a dump resulting from this condition. Message IRRE006I will follow this message with information about the return and reason codes from the RACF SIGNOFF request.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE005I THE RACF SIGNOFF REQUEST WAS UNABLE TO LOCATE USER = *userid* GROUP = *group*

Explanation: The user ID-group combination could not be located by the RACF SIGNOFF process.

System Action: The SIGNOFF command continues with requests for other APPL values if specified.

Operator Response: Verify that the SIGNOFF command was correctly entered with the desired keywords and associated operands. If the command was entered correctly and *userid* should be present, reenter the command and if the condition persists, notify your system programmer.

User Response: See the "Operator Response".

System Programmer Response: Examine the original SIGNOFF command image for possible specification errors. Examine the console logs to determine whether the specified user ID was previously signed off or some other type of abnormal condition occurred.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE006I RACROUTE TYPE=SIGNOFF REQUEST ENDED WITH A RETURN CODE OF *return-code*, REASON CODE OF *reason-code*

Explanation: This message can occur for either of the following conditions:

- The System Authorization Facility (SAF) returned a code of zero, but the RACF SIGNOFF request received an unexpected return code.
- The System Authorization Facility (SAF) received a nonzero return code that was previously shown in message IRRE004I.

System Action: The SIGNOFF command stops without further processing.

Operator Response: Notify either the system programmer or the security administrator. Note whether the SIGNOFF command has provided any previous messages and whether a system dump has been taken.

User Response: See the Operator Response.

System Programmer Response: Determine what keywords and operands are contained in the SIGNOFF command. Examine the portion of the console log

recorded before this message for the presence of other messages that might provide further information. Also, examine the system dump data sets for the presence of a dump resulting from this condition. Refer to *z/OS Security Server RACROUTE Macro Reference* for an explanation of the return code and reason code.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE007I SIGNOFF COMMAND REQUIRES THE *keyword* KEYWORD TO BE SPECIFIED

Explanation: The SIGNOFF command requires that the APPL, POE and USER keywords be specified.

System Action: The SIGNOFF command stops without further processing.

Operator Response: Reenter the command with the correct keywords.

User Response: See the Operator Response.

System Programmer Response: See the Operator Response.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE008I SIGNOFF COMMAND DOES NOT ALLOW PARTIAL GENERICS FOR THE *keyword* KEYWORD

Explanation: Partial generics (A*) were specified for the *keyword* keyword, which only allows for full generics or non-generics.

System Action: The SIGNOFF command stops.

Operator Response: Reenter the command specifying a fully qualified operand for *keyword*.

User Response: See the Operator Response.

System Programmer Response: None.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE009I SIGNOFF COMMAND COMPLETED

Explanation: This message is produced when the SIGNOFF command has completed its processing without error.

System Action: The SIGNOFF command continues to normal termination.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRE010I SIGNOFF COMMAND UNABLE TO
LOCATE APPL *APPL-name***

Explanation: The *APPL-name* specified in the APPL keyword could not be found in the table of current local LU (logical unit) names. This message is produced for explicit *APPL-name*.

System Action: The SIGNOFF command stops without further processing.

Operator Response: Check the *APPL-name* entered in the APPL keyword for being correct. Reenter the command with the proper value. If the problem persists notify the system programmer or the security administrator.

User Response: See the Operator Response.

System Programmer Response: If the *APPL-name* is known to exist in the table of current local LU names, obtain diagnostic information such as a system dump containing the table of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRE011I SIGNOFF COMMAND UNABLE TO
LOCATE A MATCH FOR APPL
*APPL-name***

Explanation: The APPL(*APPL-name*) specification was unable to find a match in the table of local LU (logical unit) names. This message is only produced when the *APPL-name* specification is of the form APPL(ABC*) or APPL(*).

System Action: The SIGNOFF command stops without further processing.

Operator Response: Check the *APPL-name* entered in the APPL keyword for being correct. Reenter the command with the proper value. If the problem persists notify the system programmer or the security administrator.

User Response: See the operator response.

System Programmer Response: If the *APPL-name* is known to match at least one entry in the table of current local LU-names, then obtain diagnostic information such as a system dump containing the table of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRE012I SIGNOFF COMMAND FOUND THAT
THERE WERE NO APPLS CURRENTLY
SIGNED ON**

Explanation: The SIGNOFF command could not successfully execute because the list of local LU (logical unit) names does not exist.

System Action: The SIGNOFF command stops without further processing.

Operator Response: No specific response is required for this message unless it is known that the list should not be empty. In that case, notify the system programmer or the security administrator.

User Response: See the Operator Response.

System Programmer Response: If this message reflects a condition that should not be present, examine the console log to determine what operations have been performed on the list of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

**IRRE080I SIGNOFF COMMAND ENCOUNTERED
AN ERROR. ABEND CODE IS
abend_code-reason_code .**

Explanation: During the normal processing of the SIGNOFF request an abnormal condition was detected. The *abend_code* and *reason_code* are displayed. Display the system dump data sets for an accompanying diagnostic dump.

System Action: The SIGNOFF command stops processing.

Operator Response: Notify the system programmer.

User Response: Notify the system programmer.

System Programmer Response: Report this message ID and its contents to your IBM support center. For a description of the abend code and reason code, refer to Chapter 8, "RACF abend codes" on page 295. If the abend code and reason code displayed in the message do not appear in this manual, refer to the system codes manual for the MVS system at your installation.

RRSF send request handling task messages

IRRF010I **RACF WAS UNABLE TO LOAD COMMUNICATION ROUTINE** (*load module*). **REMOTE RACF PROCESSING USING APPC IS DEACTIVATED.**

Explanation: The RACF subsystem address space issued the MVS macro LOAD to bring the load module into the RACF subsystem address space. This load module is needed to do any of the following:

- Issue the appropriate APPC/MVS verb
- Build a connection with another node
- Send to and receive data from a remote node
- Process requests for the local node

System Action: No attempt is be made to register as an APPC/MVS server or to activate connections to other nodes. The local node processing is not activated. Any TARGET command requests to change the state of the connection to other nodes are ignored. The RACF subsystem address space saves the request that was issued. After the connection is made, RACF sends the request to the indicated node.

Operator Response: Determine why the requested load module could not be found and loaded into the RACF subsystem address space. When the problem has been corrected, issue the RESTART CONNECTION command. This causes the RACF subsystem address space to attempt to bring the needed load modules into the RACF subsystem address space.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRF080I *subsystem-name* **SUBSYSTEM SEND REQUEST HANDLING TASK ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*.

Explanation: The SEND request task was routing a work request to its destination on another node. This message appears when an abnormal event occurs. This message is written to the SYSLOG.

System Action: The SEND handler attempts to retry the current work request.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of ABEND, the subtask should resume processing any work in its input queue. Refer to “Actions to Recover from an RRSF Failure” in *z/OS Security Server RACF Diagnosis Guide* for a complete discussion.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: See *z/OS MVS System Codes* for an explanation of these codes.

IRRF081I *subsystem-name* **SUBSYSTEM SEND REQUEST HANDLING TASK ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*. **SEND REQUEST TASK ENDING.**

Explanation: The SEND request task was routing a work request to its destination on another node. This message appears when an abnormal event occurs.

System Action: The SEND handler releases system resources it holds and ends processing.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of ABEND, the subtask should resume processing any work in its input queue. Refer to “Actions to Recover from an RRSF Failure” in *z/OS Security Server RACF Diagnosis Guide* for a complete discussion.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: See *z/OS MVS System Codes* for an explanation of these codes. The task that started the SEND request task attempts to restart the task. Verify that message IRRB020I was issued showing that the task restart was successful.

Destination: Descriptor code is 6. Routing code is 2.

RRSF PARMLIB and initialization messages

IRRG001I *subsystem-name* **SUBSYSTEM UNABLE TO OPEN MEMBER IRROPT_{yy} IN THE RACF PARAMETER LIBRARY.**

Explanation: OPEN processing failed on the indicated subsystem for member IRROPT_{yy} of the RACF parameter library. No configuration statements from this member of the RACF parameter library will be processed.

System Action: None.

Operator Response: Report the text of this message to the system programmer.

System Programmer Response: If the RACF parameter library member appears to be valid, report the occurrence of the error to the IBM support center.

Destination: Descriptor code is 6. Routing code is 2.

Security Server RACF System Programmer's Guide.

Once the necessary updates have been made, the RACF subsystem can be stopped and restarted to activate your changes.

For example, if your RACF subsystem name is 'RACF' and its (optional) subsystem identifier is '@', then from the operator console you would issue

```
@STOP
START RACF,SUB=MSTR,PARM='OPT=xx'
```

Alternatively, you could issue the SET and TARGET commands in the IRROPT_{xx} member manually, although this is not the recommended method.

Unless the JCL is updated, this message will appear again.

Destination: Descriptor code is 6. Routing code is 2.

IRRG002I *subsystem-name* **SUBSYSTEM COULD NOT LOCATE THE RACFPARM DD STATEMENT FOR THE RACF PARAMETER LIBRARY DATA SET.**

Explanation: This message is displayed for one of the following reasons:

- You specified PARM='OPT=xx' on the EXEC JCL statement in the RACF procedure in SYS1.PROCLIB. However, you did not also supply the RACFPARM DD statement to identify the RACF parameter library data set containing the IRROPT_{xx} member.
- You issued a SET INCLUDE(xx) command when the RACFPARM DD statement does not exist.

Because RACF cannot locate this data set, the commands contained within the IRROPT_{xx} member are not processed. Therefore, if this message was displayed during RACF subsystem address space initialization, the RACF remote sharing facility is not activated.

System Action: If this message was displayed during RACF subsystem address space initialization, initialization continues without activating RRSF. Any updates you make to the RACF database are not propagated to any other RACF database in your RRSF configuration until the problem is resolved. If the message was issued as a result of a SET INCLUDE(xx) command entered as an operator command, the command simply ends.

Operator Response: Contact your system programmer.

System Programmer Response: The started procedure for the RACF subsystem in SYS1.PROCLIB must be updated to provide the RACFPARM DD statement, which identifies the data set that contains the IRROPT_{xx} member. For information on how to update your started procedure for remote sharing, see *z/OS*

IRRG005I *subsystem-name* **SUBSYSTEM UNABLE TO LOCATE IRROPT_{yy} IN RACFPARM.**

Explanation: The RACF parameter library data set does not contain the member IRROPT_{yy} that was to be processed by the indicated subsystem.

System Action: The intended configuration statements are not processed.

Operator Response: If the message occurs because you issued a SET INCLUDE(yy) command, reissue a corrected form of the command. If the message occurs during the RACF parameter library processing portion of subsystem initialization, report the complete text of the message to the system programmer.

System Programmer Response: Check the RACF parameter library members for their existence and validity. Pay particular attention to member references made by SET INCLUDE() statements.

Destination: Descriptor code is 6. Routing code is 2.

IRRG006I **A COMMAND IN PARAMETER LIBRARY MEMBER IRROPT_{yy} HAS EXCEEDED THE MAXIMUM OF *number* CONTINUATION LINES.**

Explanation: Commands to be processed from the RACF parameter library must not exceed *number* continuation lines. A parameter library command that exceeds this limit was detected and was not processed.

System Action: None

Operator Response: See accompanying message IRRG007I for an indication of which command was in error.

Destination: Descriptor code is 6. Routing code is 2.

IRRG007I • IRRG012A

IRRG007I **THE FIRST PORTION OF THE
COMMAND IS:** xxxxxxxxxxxxxxxxxxxx.

Explanation: xxxxxxxxxxxxxxxxxxxx is the first portion of the command that was ignored due to its excessive length. See preceding message IRRG006I.

System Action: None.

Operator Response: Report the text of this message to the system programmer.

System Programmer Response: Shorten the command, or remove it from the RACF parameter library.

Destination: Descriptor code is 6. Routing code is 2.

IRRG008I *subsystem-name* **SUBSYSTEM IS
PROCESSING PARAMETER LIBRARY
MEMBER IRROPT_{yy}.**

Explanation: This message indicates that processing of the IRROPT_{yy} member of the RACF parameter library was begun by the indicated subsystem.

System Action: Configuration statements (commands) within the RACF parameter library member are read and processed.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRG009I *subsystem-name* **SUBSYSTEM CANNOT
PROCESS PARAMETER LIBRARY
MEMBER IRROPT_{yy} RECURSIVELY.**

Explanation: One or more recursive references to RACF parameter library member IRROPT_{yy} have been detected during parameter library processing by the indicated subsystem. The recursive references are not processed. However, other RACF parameter library processing continues.

System Action: None.

Operator Response: Report the text of this message to the system programmer.

System Programmer Response: Remove all recursive references from the RACF parameter library.

Destination: Descriptor code is 6. Routing code is 2.

IRRG010I *subsystem-name* **SUBSYSTEM
PROCESSING OF PARAMETER
LIBRARY MEMBER IRROPT_{yy} IS
COMPLETE.**

Explanation: This message indicates that processing of the IRROPT_{yy} member of the RACF parameter library was completed by the indicated subsystem.

System Action: None.

Operator Response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRG011I **THE LAST COMMAND IN PARAMETER
LIBRARY MEMBER IRROPT_{yy} WAS
IGNORED BECAUSE OF INCORRECT
CONTINUATION.**

Explanation: The last command to be processed from a RACF parameter library member must not end with a continuation character. The command is considered incomplete and is not processed.

System Action: None.

Operator Response: See accompanying message IRRG007I for an indication of which command was in error.

Destination: Descriptor code is 6. Routing code is 2.

IRRG012A **INCORRECT VERSION OF RACF
ENABLED IN IFAPRD_{xx}.**

Explanation: The active IFAPRD_{xx} members of SYS1.PARMLIB contain a PRODUCT entry that enables the RACF product (5695-039) but not the z/OS Security Server feature. Starting with OS/390 Release 3, the RACF function was shipped only as a part of the OS/390 Security Server feature. The RACF function can be used only when it is ordered and enabled as the z/OS Security Server feature.

System Action: The RACF component of the z/OS Security Server initializes to provide you with a system you can use to correct the IFAPRD_{xx} entries for RACF and the z/OS Security Server feature. During initialization, RACF registers as the z/OS Security Server, not as the RACF product.

System Programmer Response: Correct the IFAPRD_{xx} entries according to your licensing agreements and IPL the system.

- If the z/OS Security Server feature has already been ordered, change the Security Server feature's STATE value to ENABLED in the appropriate IFAPRD_{xx} member.
- If the RACF function is required but the OS/390 Security Server feature was not ordered, order the feature from IBM and change its STATE value to ENABLED.
- If neither the RACF nor DCE Security Server functions are required, do one of the following:
 - Remove the RACF (5695-039) entry from the appropriate IFAPRD_{xx} member
 - Change its STATE value to DISABLED

For additional information, see *z/OS MVS Product Management*.

Destination: Descriptor code is 2. Routing code is 1.

IRRG080I *subsystem-name* **SUBSYSTEM
PARAMETER LIBRARY HANDLING
ENCOUNTERED AN ERROR. ABEND
CODE IS** *returncode-reasoncode*.

Explanation: RACF parameter library processing ended abnormally for the indicated subsystem, with the given return and reason codes. This message is written to the SYSLOG.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

SET command messages

IRRH001I *subsystem-name* **SUBSYSTEM SET
COMMAND ENDED IN RECURSIVE
ABEND.**

Explanation: The SET command abnormally ended in its attempt to recover from a prior abend on the indicated subsystem.

System Action: None.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

Destination: Descriptor code is 6.

IRRH004I *subsystem-name* **SUBSYSTEM SET
COMMAND HAS COMPLETED
SUCCESSFULLY.**

Explanation: The SET command was processed by the *subsystem-name* subsystem without any errors.

System Action: None.

Operator Response: None.

Destination: Descriptor code is 6.

IRRH002I *subsystem-name* **SUBSYSTEM SET
COMMAND ENDED IN ERROR.**

Explanation: The SET command encountered an error during processing on the indicated subsystem. See any accompanying messages for more specific error information.

System Action: None.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center if the accompanying error messages do not indicate user error.

Destination: Descriptor code is 6.

IRRH005I *subsystem-name* **SUBSYSTEM
INFORMATION:**

Explanation: This message precedes the remainder of the output displayed by SET LIST processing.

Operator Response: None.

Destination: Descriptor code is 6.

IRRH006I **MORE THAN FOUR USERS WERE
SPECIFIED WITH THE OUTPUT AND
NOTIFY KEYWORDS ON THE SET
COMMAND.**

Explanation: On the SET command, more than four users were specified with the OUTPUT and NOTIFY keywords. The combination of users specified on the two keywords can be a maximum of four *different* users. In other words, the cumulative total of unique users may not exceed four in both the OUTPUT and NOTIFY keywords. The same four users may be specified on each keyword. However, if four users are specified on one of the keywords, a (different) fifth user may not be specified on the other keyword. For example, if four users are specified on the OUTPUT keyword, a fifth user may not be specified on the NOTIFY keyword.

System Action: Command processing fails to complete.

User Response: Issue the command again, specifying no more than four different users with the OUTPUT and NOTIFY keywords.

Destination: Descriptor code is 6.

IRRH003I **ISSUER HAS INSUFFICIENT
AUTHORITY TO KEYWORD** *keyword* **ON**
subsystem-name **SUBSYSTEM SET
COMMAND.**

Explanation: RACF OPERCMDS class profiles currently fail to authorize the command issuer to use the named keyword with the SET command when invoking its processing by the *subsystem-name* subsystem.

System Action: The SET command ends in error.

Operator Response: Contact your RACF security administrator to obtain the proper authority.

IRRH007I *operand* **SPECIFIED ON THE { ALWAYS | WARN | FAIL } KEYWORD OF THE SET COMMAND IS NOT VALID.**

Explanation: On the indicated SET command keyword, an operand was specified with incorrect syntax. The correct syntax is any of the following:

- *node.userid*
- *.userid*
- &RACUID

System Action: Command processing fails to complete.

User Response: Issue the command again, correcting the operand which is in error.

Destination: Descriptor code is 6.

IRRH008I **THE SET COMMAND HAS RESTORED THE PREVIOUS SETTINGS OF THE OUTPUT AND NOTIFY KEYWORDS.**

Explanation: The SET AUTODIRECT command was issued with no values specified for the OUTPUT and NOTIFY keywords. When a previous SET NOAUTODIRECT command was issued, the settings of the OUTPUT and NOTIFY keywords were saved. These settings have now been restored.

System Action: Command processing continues.

User Response: The user can issue the SET LIST command to display the restored settings.

Destination: Descriptor code is 6.

IRRH009I **WARNING! THE SET COMMAND HAS ACTIVATED *rrsf_function* BUT NO USERS HAVE BEEN SPECIFIED ON THE OUTPUT OR NOTIFY KEYWORDS.**

Explanation: The *rrsf_function* AUTODIRECT, AUTOPWD, PWSYNC, or AUTOAPPL was issued with no values specified for the OUTPUT and NOTIFY keywords. If errors occur during automatic command direction, no one is notified of the errors, and RACF profiles do not remain synchronized.

If the SET AUTODIRECT command was issued with the intent of restoring previous settings of the OUTPUT and NOTIFY keywords, no saved settings were found and, therefore, could not be restored.

System Action: Command processing continues.

User Response: If the intention was to have someone notified when errors occur during automatic command direction, issue the command again, specifying at least one user on the OUTPUT or NOTIFY keyword.

Destination: Descriptor code is 6.

IRRH080I *subsystem-name* **SUBSYSTEM SET COMMAND ENCOUNTERED AN ERROR. ABEND CODE IS *returncode-reasoncode*.**

Explanation: The SET command processed by the *subsystem-name* subsystem ended abnormally, with the given return and reason codes.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRH082I **THE TRACE KEYWORD REQUIRES ADDITIONAL SPECIFICATION.**

Explanation: The TRACE keyword requires the specification of 1 or more of its options.

System Action: The SET command ends in error.

Operator Response: Reissue a corrected version of the command, if necessary. See *z/OS Security Server RACF Command Language Reference* for the syntax of the SET command.

Destination: Descriptor code is 6.

RRSF handshaking messages

IRRI000I **LOCAL RACF NODE** *local-node*
[SYSNAME *system-name* **] IS**
ATTEMPTING TO CONTACT PARTNER
RACF NODE *partner-node* **[SYSNAME**
system-name **].**

Explanation: This is an informational message only. One or more RACF TARGET commands were issued at the local RACF node *local-node* that caused it to attempt to establish communications with the partner node *partner-node*. The local node waits for a response from the partner (the partner should issue its own TARGET command). Once the partner has responded, information is exchanged and an attempt is made to open up RACF communication between these two nodes. This is known as entering the OPERATIVE ACTIVE state. This message is written to the SYSLOG. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

System Programmer Response: If you receive this message and do not get a response either confirming or denying communication, ensure that the partner RACF node did issue a TARGET statement for this node (with the correct LU name). A TARGET NODE(*node-name*) LIST command can be issued on the partner node to list the node definition as it is defined here. You should also check for communication protocol failures (that is, APPC), because that is the means RACF is using to communicate with the partner.

IRRI001I **RACF COMMUNICATION WITH NODE**
partner-node **[SYSNAME** *system-name* **]**
HAS BEEN SUCCESSFULLY
ESTABLISHED.

Explanation: This is an informational message only. One or more RACF TARGET commands were issued that caused RACF to establish this communication link with the partner node. RACF on each node has successfully exchanged information and both have agreed to allow the communication. Communication is now considered OPERATIVE ACTIVE between these two nodes. If SYSNAME information is present in this message, the partner node *partner-node* is a multisystem node.

System Programmer Response: No response is needed if you expected RACF to be communicating with RACF on the partner node. Otherwise, you might want to issue RACF TARGET commands to remove the communication path or modify the RACF parameter library commands that you currently run during RACF subsystem initialization.

Destination: Descriptor code is 6. Routing code is 2.

IRRI004I **ATTENTION: LOCAL NODE** *local-node*
[SYSNAME *system-name* **] HAS**
TEMPLATE VERSION *xxxxxxx*.
PARTNER NODE *partner-node*
[SYSNAME *system-name* **] HAS**
TEMPLATE VERSION *xxxxxxx*.

Explanation: This is an attention message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. The template level is an example of this data and a mismatch has been detected. Adding a field on one node may work, but fail on the other node until the corresponding template update takes place on that node. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

System Action: If no error messages are issued with this attention message, RACF still attempts to move this node pair into the OPERATIVE ACTIVE state. Message IRRI001I tells you when the OPERATIVE ACTIVE state is reached.

System Programmer Response: Evaluate the template levels in the message. If you do not plan to add or alter a profile specifically using the fields in the more recent version of the templates, you may ignore this message until the next service upgrade causes the templates to match. If you plan to use the new fields, you need to correct the template mismatch by running the IRRMIN00 utility on the downlevel node, then IPL that node. Remember to upgrade the RACF dynamic parse specification data set (IRRDPSDS) to match the template level. When the template levels match, you will no longer see this message when the two nodes TARGET each other.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI005I **ATTENTION: LOCAL NODE** *local-node*
[SYSNAME *system-name* **] HAS**
DYNAMIC PARSE VERSION *xxxxxxx*.
PARTNER NODE *partner-node*
[SYSNAME *system-name* **] HAS**
DYNAMIC PARSE VERSION *xxxxxxx*.

Explanation: This is an attention message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. The dynamic parse specification data (IRRDPSDS) level is one of these types of data and a mismatch has been detected. Adding a profile segment field on one node may work, but fail on the other node until the corresponding dynamic parse specification update takes place on that

IRRI006I • IRRI007I

node. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

This message also occurs if dynamic parse initialization has not completed on both nodes. The dynamic parse version displayed for a node that has not completed dynamic parse initialization is '<UNKNOWN>'.

System Action: If no error messages are issued with this attention message, RACF still attempts to move this node pair into the OPERATIVE ACTIVE state. Message IRRI001I will confirm when the OPERATIVE ACTIVE state is reached.

System Programmer Response: Evaluate the dynamic parse levels in the message. If you do not plan to add or alter a profile specifically using the segment fields which exist in the more recent version of the IRRDPSDS, you may ignore this message until the next service upgrade causes the members to match. If you plan to use the new fields, you need to correct the IRRDPSDS mismatch by running the IRRDPI00 UPDATE command on the down level node. Remember to upgrade the RACF templates to match the dynamic parse level. When the IRRDPSDS levels match, you will no longer see this message when the two nodes TARGET each other.

If this message occurred because dynamic parse initialization did not complete on both nodes, dynamic parse initialization can be performed prior to starting the RACF address space to reduce the likelihood of this message appearing. After dynamic parse has completed on both nodes, SET LIST can be issued on each node to display the dynamic parse level. Alternatively, a command such as TARGET NODE(*local-node*) OP that causes RACF to re-examine dynamic parse levels on both nodes can be issued. If the dynamic parse levels do not match, message IRRI005I is displayed again.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI006I **WARNING: LOCAL NODE** *local-node*
HAS SETROPTS OPTION *option*.
PARTNER NODE *partner-node* **HAS**
SETROPTS OPTION *option*.

Explanation: This is a warning message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. The indicated SETROPTS option is one of these types of data and a mismatch has been detected. Adding a profile on one node may work, but fail on the other node until the corresponding SETROPTS options match.

System Action: If no error messages are issued with this warning message, RACF still attempts to move this node pair into the OPERATIVE ACTIVE state. Message IRRI001I tells you when the OPERATIVE ACTIVE state is reached.

System Programmer Response: Evaluate the SETROPTS options in the message. IBM recommends that these SETROPTS options match when you wish two RACF nodes to communicate with each other. You should use the SETROPTS command to change one or both nodes so that the SETROPTS options match. When the SETROPTS options match, you will no longer see this message when the two nodes TARGET each other.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI007I **WARNING: LOCAL NODE** *local-node*
HAS A DIFFERENT SETROPTS
PASSWORD(RULEx) THAN PARTNER
NODE *partner-node*.

Explanation: This is a warning message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. The SETROPTS PASSWORD(RULEx) is one of these types of data and a mismatch has been detected. As a result, a change in password may be accepted on one node but rejected on the other node unless the SETROPTS password rules match.

When the password rules are the same, they do not need to be listed in the same order on both nodes.

System Action: If no error messages are issued with this warning message, RACF still attempts to move this node pair into the OPERATIVE ACTIVE state. Message IRRI001I tells you when the OPERATIVE ACTIVE state is reached.

System Programmer Response: Evaluate the SETROPTS password rule listed in the message. IBM recommends that these SETROPTS password rules be consistent when you wish two RACF nodes to communicate with each other. You should use the SETROPTS command to change one or both nodes so that the SETROPTS password rules are consistent. If you plan to allow RACF to synchronize passwords between these nodes, it is recommended that the existing sets of password rules be merged into a single set that contains the most restrictive of the original rules. Both nodes should then use this new set of rules. This prevents acceptable passwords on one node from failing on a more restrictive node. When the SETROPTS options are consistent, you will no longer see this message when the two nodes TARGET each other.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI011I **ERROR: LOCAL NODE** *local-node*
[SYSNAME *system-name***] HAS RACF**
LEVEL *xxxxx*. **PARTNER NODE**
partner-node **[SYSNAME** *system-name***]**
HAS RACF LEVEL *xxxxx*.

Explanation: This is an error message. The RACF levels at local node *local-node* and its partner node *partner-node* are not compatible. Each node needs to be at RACF 2.2 or higher in order for communication to occur between the nodes. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

System Action: Because this is an error, RACF does not move this node pair into the OPERATIVE ACTIVE state, but leaves them in an OPERATIVE PENDING VERIFICATION state. Message IRRI013I indicates that RACF is not communicating with the partner node.

System Programmer Response: Evaluate the RACF levels in the message. Upgrade your RACF level and retry the request. See *z/OS Security Server RACF System Programmer's Guide* for additional information. When the RACF levels match at RACF 2.2 or higher, you will no longer see this message when the two nodes TARGET each other, and communication should be allowed between the nodes.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI012I **ERROR: LOCAL NODE** *local-node*
[SYSNAME *system-name***] HAS**
PROTOCOL LEVEL *xxxxx*. **PARTNER**
NODE *partner-node* **[SYSNAME**
*system-name***] HAS PROTOCOL LEVEL**
xxxxx.

Explanation: RACF checks certain data between the partner node and the local node to determine if they are compatible enough to allow communication between the nodes. The transportation protocol level is a crucial condition and has been found to be at incompatible levels. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

System Action: RACF does not move this node pair into the OPERATIVE ACTIVE state, but leaves them in an OPERATIVE PENDING VERIFICATION state. Message IRRI013I indicates that RACF is not communicating with the partner node.

System Programmer Response: The transportation protocol values should always match. However, it is possible that PTF service to RACF modules could introduce a condition where RACF cannot tolerate communication between certain different service levels. Important load modules that could affect this are IRRDDM00, IRRAPPC0, IRRAPPC2, and IRRAPPC6. If you receive this message, you should check PTFs that

affect CSECTs in these load modules and see if there was hold information that recommended the PTF be applied to all communicating systems at the same time. If so, apply the PTF on the remaining systems and TARGET the nodes operative again. If this does not correct the problem, contact the IBM support center.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI013I **RACF COMMUNICATION WITH NODE**
partner-node **[SYSNAME** *system-name***]**
HAS BEEN REJECTED.

Explanation: This message indicates RACF has denied communication with RACF on the partner node. Information was found to be incompatible, and RACF did not open up communication between this node and the partner node. If SYSNAME information is present in this message, the partner node *partner-node* is a multisystem node.

System Action: These two nodes are left in the OPERATIVE PENDING VERIFICATION state. Communication is not allowed between these two nodes.

System Programmer Response: Refer to any preceding RACF error messages to determine what was incompatible between the two nodes. Correct the RACF differences and TARGET the nodes operative again.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI014I **ERROR: LOCAL NODE** *node-name*
[SYSNAME *system-name***] AND**
PARTNER NODE *node-name* **[SYSNAME**
*system-name***] HAVE CONFLICTING**
TARGET STATEMENTS WITH {LOCAL |
REMOTE} LUNAME *luname*. **REASON**
CODE *reason-code*.

Explanation: RACF has successfully made a connection between the local node and a remote LU name. However, there is an inconsistency in the TARGET statements on the local and remote sides about what one of those LU names reference. The text of this message indicates the LU name in conflict and the reason code indicates the inconsistency. The reason code is one of these values:

Reason

- 1** There is no agreement on node-name.
- 2** There is no agreement whether a node is a multisystem node or a single-system node.
- 3** There is no agreement on system-name.
- 4** There is no agreement whether the system on the multisystem node is the MAIN system.

System Action: Because these are errors, RACF will not move this node pair into the OPERATIVE-ACTIVE state. Instead they will be left in an OPERATIVE-PENDING-VERIFICATION state. You will

IRRI015I • IRRI081I

see message IRRI013I indicating that RACF will not be communicating with the partner node.

Operator Response: Do the following:

- Issue the TARGET LIST command from both nodes and determine the error. If a node is multisystem, ensure the TARGET LIST command is done from the specific system involved.
- Issue the TARGET DELETE command for the incorrect node definitions and TARGET the correct ones. If a node is multisystem, ensure the corrections are made on every system.
- Ensure corresponding updates are made to the RACF parameter library for future refreshes of the subsystem or relPLs.

Destination: Descriptor code is 6. Routing code is 2.

IRRI015I **ERROR: HANDSHAKING HAS ALREADY FAILED ON PARTNER RRSF NODE** *node-name* [SYSNAME *system-name*].

Explanation: An attempt has already been made to make this partner RRSF node operative and handshaking failed. Handshaking is not reattempted.

System Action: These two nodes are left in the OPERATIVE PENDING VERIFICATION state. Communication is not allowed between these two nodes.

System Programmer Response: Refer to any preceding RACF error messages to determine what was incompatible between the two nodes. If message IRRI014I was issued, correct the problem and issue RESTART CONNECTION for the specific node or system. If a protocol mismatch is detected, the entire APPC server task must be restarted to reload all handshaking modules. This can be done by issuing RESTART CONNECTION without the NODE keyword. If incompatible RACF levels are detected, an IPL is required after upgrading to a compatible RACF level to correct the problem.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI080I *subsystem-name* **SUBSYSTEM APPC HANDSHAKING TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*.

Explanation: The handshaking task was processing conversation connection parameters. This message appears when an abnormal event occurs.

System Action: The handshaking task attempts to retry the current work request. If the retry does not work, message IRRI081I is issued.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these

codes, see *z/OS MVS System Codes*.

Destination: Descriptor code is 1. Routing codes are 2 and 9.

IRRI081I *subsystem-name* **SUBSYSTEM APPC HANDSHAKING TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*. **HANDSHAKING TASK ENDING.**

Explanation: The handshaking task was processing conversation connection parameters. This message appears when an abnormal event occurs.

System Action: The handshaking subtask ends and the parent task attempts to restart the handshaking subtask.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

Destination: Descriptor code is 6. Routing code is 2.

RRSF connection local transaction program messages

IRRJ000I *subsystem-name* **RACF LOCAL NODE TRANSACTION PROGRAM STARTING UNDER USER ID *userid* GROUP *group-name*.**

Explanation: This message goes to the SYSLOG when the local node transaction program completes its initialization. The local RACF subsystem can process commands sent to it for processing on the local system.

IRRJ001I *subsystem-name* **RACF LOCAL NODE TRANSACTION PROGRAM COMPLETED UNDER USER ID *userid* GROUP *group-name*.**

Explanation: This message goes to the SYSLOG when the local node transaction program stops processing. The program may be stopped as a result of an operator request to make the node dormant or as the result of a operational error. Earlier messages may indicate the nature of the problem.

System Action: The RACF subsystem does not run any local work until the node is returned to operative active status. Additional RACF commands directed to the local node are held in the local OUTMSG workspace data set. Work (commands and other requests) active in the RACF address space continue to run. Work directed to other nodes continues to be processed if the target node is operative active.

Operator Response: Review the console log for an indication of the original error.

IRRJ080I *subsystem-name* **RACF LOCAL NODE TRANSACTION PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS *abend-code*.**

Explanation: A local node transaction program handling work requests to run in the RACF subsystem had an error. This message appears every time an abnormal event occurs. This message is written to the SYSLOG.

System Action: The transaction program attempts to restart work requests from the local INMSG workspace data set and from the local OUTMSG workspace data set. If an abend occurs during this processing, the program discards the record and reads the next record in the data set.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. Refer to “Actions to Recover from an RRSF Failure” in for a complete discussion. *z/OS Security Server RACF Diagnosis Guide*

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

IRRJ081I *subsystem-name* **RACF LOCAL NODE TRANSACTION PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS *abend-code*. PROGRAM ENDING.**

Explanation: A local node transaction program handling work requests to run in the RACF subsystem had an error. This message appears when the program encounters an abnormal event that cannot be recovered from.

System Action: The transaction program cannot recover from this abnormal error. The program releases all system resources it holds and then ends. The node connection program attempts to restart the local transaction program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. Refer to “Actions to Recover from an RRSF Failure” in *z/OS Security Server RACF Diagnosis Guide* for a complete discussion.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

Destination: Descriptor code is 6. Routing code is 2.

RACLINK command messages

IRRK080I *subsystem-name* **SUBSYSTEM RACLINK
TASK HAS ENCOUNTERED AN
ERROR. ABEND CODE IS** *abend-code*.

Explanation: The RACF subsystem RACLINK task has abended for the indicated subsystem. This message is written to the SYSLOG.

System Action: The RACF subsystem continues processing without this RACLINK task.

Operator Response: Take the steps indicated by for *z/OS MVS System Codes* the abend and reason code that was displayed when the subtask abended. Once the problem has been resolved, restart the RACLINK subtask using the RESTART command.

RACROUTE REQUEST=LIST messages

IRRL0000I Error occurred while processing RACGLIST profile *classname_nnnnn*, error code = *error*, RACF manager return code = *retcode*, reason code = *rsncode*.

Explanation: While RACF was processing RACGLIST profiles, an error was encountered while processing the *classname_nnnnn* profile. *Error* uniquely identifies where in RACF the problem was discovered.

System Action:

- If the problem occurred while RACF was building a RACLIST data space from the RACGLIST profiles, RACF reverts to standard RACLIST processing, which loads the original class profiles from the database into a data space instead of using the RACGLIST profiles. The RACGLIST *classname_nnnnn* profiles are rebuilt.
- If the problem occurred while saving the RACLIST data space contents on the database as RACGLIST profiles, RACLIST processing has created the data space successfully, but the contents were not saved as RACGLIST profiles. An attempt is made to delete all *classname_nnnnn* profiles from the RACF database. If a second IRRL0000I message is not issued, the attempt was successful and all but the base *classname* profile were deleted.
- If the problem occurred while deleting the RACGLIST profiles, for example, during a SETR NORACLIST or RDELETE command, all the RACGLIST profiles may not have been deleted.

In all cases, an SVC dump is taken.

Operator Response: Notify the system programmer.

System Programmer Response:

1. Look up RACF manager return and reason codes in "RACF Manager Return Codes" on page 307 to determine the cause.
2. Issue SEARCH CLASS(RACGLIST) to determine the status of the RACGLIST profiles.
3. Issue a SETROPTS RACLIST REFRESH for the indicated *classname* to rebuild RACGLIST profiles or RDELETE the offending profile(s).
4. If the problem persists, report the problem to the IBM support center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL0001I Error occurred while processing RACGLIST profile *classname_nnnnn*, error code = *error*.

Explanation: While RACF was building a RACLIST data space from the RACGLIST profiles, an error was encountered while processing the *classname_nnnnn*

profile. *Error* uniquely identifies where in RACF the problem was discovered.

System Action: RACF reverts to standard RACLIST processing, which loads the original class profiles from the database into a data space instead of using the RACGLIST profiles. The RACGLIST *classname_nnnnn* profiles are rebuilt.

Operator Response: Notify the system programmer.

System Programmer Response: Issue a SETROPTS RACLIST REFRESH for the indicated *classname* to rebuild RACGLIST profiles. If the problem persists, report the problem to the IBM support center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL0002I RACROUTE REQUEST=LIST for *classname* failed to build or return a data space, error code = *error*.

Explanation: A RACROUTE REQUEST=LIST, GLOBAL=YES, for class *classname* has failed. The error code uniquely identifies where in RACF the problem was discovered.

System Action: The RACLIST failed with SAF return code = X'8', RACF return code = X'24', RACF reason code = X'0'. Under some circumstances, an SVC dump is taken.

Operator Response: Notify the system programmer.

System Programmer Response: Report the problem to the IBM support center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL0003I RACLIST of class *classname* failed. {Profile | Grouping Class Profile | Group Member} *pname* is too large.

Explanation: While processing a SETROPTS RACLIST [REFRESH] or RACROUTE REQUEST=LIST request for a class, the in-storage profile *pname* being built from one of the following was too large to be RACLISTed:

- A profile in class *classname*
- A profile in the grouping class associated with *classname*
- A member of one or more grouping class profiles associated with *classname*

If *pname* is followed by the notation '(G)', it is a generic profile.

System Action: The RACLIST [REFRESH] request failed with SAF return code = X'08', RACF return code = X'0C', RACF reason code = X'00'.

IRRL1000I • IRRL1001I

User Response: The in-storage profile *pname* was too large to be RACLISTed.

If the profile is defined to RACF in more than one way, for example, as a member of a grouping class profile and as a profile in the corresponding member class, RACF merges the multiple definitions to form a resulting in-storage profile. It may be the combination of the two or more definitions of the profile, not the individual definitions themselves, that caused the profile to be too large.

If *pname* is identified as a group member in the message, you can issue the RLIST *classname pname* RESGROUP command to locate all the grouping class profiles that have it as a member.

Decrease the size of the profile (or its associated profiles). The standard and conditional access lists are the most likely areas to cause the profile to grow. Other areas to consider are the installation data, the application data, or categories.

After you have made the profile smaller, reissue the

SETROPTS RACLIST command or have the application reissue the RACROUTE REQUEST=LIST request. If the profile is generic, issue the SETROPTS GENERIC(*classname*) REFRESH command.

Note: If you are not responsible for administrating those profiles, you should contact the RACF security administrator.

For more information on the size restriction of an in-storage profile, see the section in the *z/OS Security Server RACF Security Administrator's Guide* on "Limiting the Size of Your Access Lists".

Operator Response: Report this message to the RACF security administrator.

System Programmer Response: See User Response.

Destination: Descriptor code is 6. Routing codes are 2 and 11.

CACHECLS profile messages

IRRL1000I **Cache is intact. Error occurred while processing CACHECLS profile**
profile-name, **error code = error**, **RACF manager return code = retcode**, **reason code = rsnocode**.

Explanation: An R_cacheserv callable service was invoked. During the hardening of the cache contents to the RACF database as CACHECLS profiles, an error occurred while processing profile *profile-name*. *Profile-name* is in the format of either '*cachename*' or '*cachename_ddd_nnnnn*', where *cachename* is the value of the Cache_Name parameter on the R_Cacheserv callable service. '*ddd*' and '*nnnnn*' are the dataspace number and sequential number respectively (both in decimal) of one of the profiles holding the contents of that particular dataspace. *Error* is provided to assist IBM support personnel in identifying where in RACF the problem was discovered. RACF manager return and reason codes (in hexadecimal) are also provided to further delineate the problem.

The local cache is intact, but may not have been hardened to the database correctly. The application using the cache should not be affected now, but after an IPL it may not be possible to restore the cache from information on the RACF database. In that case, the application would not have use of the cache until it was built by other means.

System Action: RACF attempts to delete all the *cachename_ddd_nnnnn* profiles. If message IRRL1002I is not issued, the attempt was successful. If an IRRL1002I message is issued, then all *cachename_ddd_nnnnn* profiles may not have been deleted.

Additionally, a symptom record for the error is created and stored in the LOGREC data set.

Operator Response: Notify the System Programmer.

System Programmer Response:

1. Look up the RACF manager return and reason codes on page "RACF Manager Return Codes" on page 307 to determine the cause of the problem.
2. Contact your Security Administrator to check the status of the *cachename_ddd_nnnnn* profiles.

Security Administrator Response:

If IRRL1002I is issued, then:

- Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS *cachename_ddd_nnnnn* profiles
- If some remain, delete those profiles with the RACF RDELETE command.
- If the problem persists, report the problem to the IBM Support Center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL1001I **Cache is not created. Error occurred while processing CACHECLS profile**
profile-name, **error code = error** {, **RACF manager return code = retcode**, **reason code = rsnocode**}.

Explanation: An R_cacheserv callable service was invoked. When RACF was building a cache from profiles on the RACF database in the CACHECLS class, an error was encountered while processing profile *profile-name*. *Profile-name* is in the format of either

'cachename', or 'cachename_ddd_nnnnn', where *cachename* is the value of the Cache_name parameter on the R_Cacheserv callable service 'ddd' and 'nnnnn' are the daspace number and sequential number respectively (both in decimal) of one of the profiles holding the contents of that particular daspace. *Error* is provided to assist IBM support personnel in identifying where in RACF the problem was discovered. RACF manager return and reason codes (in hexadecimal) are provided if the problem was encountered while accessing the RACF database.

System Action: The local cache is not created, which means that applications cannot utilize the cache. Also, an attempt was made to delete all *cachename_ddd_nnnnn* profiles from the RACF database. If an IRRL1002I message is not additionally issued, the attempt was successful and all *cachename_ddd_nnnnn* profiles have been deleted. If an IRRL1002I message is issued, then all *cachename_ddd_nnnnn* profiles may not have been deleted.

Additionally, a symptom record for the error is created and stored in the LOGREC data set.

Operator Response: Notify the System Programmer.

System Programmer Response:

- Look up the RACF manager return and reason codes on page "RACF Manager Return Codes" on page 307 to determine the cause of the problem.
- Contact your Security Administrator to check the status of the *cachename_ddd_nnnnn* profiles.

Security Administrator Response:

- Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS *cachename_ddd_nnnnn* profiles
- If some remain, delete those profiles with the RACF RDELETE command.
- If the problem persists, report the problem to the IBM Support Center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL1002I Delete request problem. Error occurred while processing CACHECLS profile *profile-name*, scope = [ddd][MULTI][ALL], error code = *error*, RACF manager return code = *retcode*, reason code = *rsncode*

Explanation: RACF was processing a request to delete CACHECLS profiles due to an RDELETE command or an R_cacheserv callable service invocation, and encountered an error while processing profile *profile-name*. *Profile-name* is in the format of either 'cachename', or 'cachename_ddd_nnnnn', where *cachename* is the value of the Cache_Name parameter on the R_Cacheserv callable service. 'ddd' and 'nnnnn' are the daspace number and sequential number (both

in decimal) of one of the profiles holding the contents of that particular daspace. The scope of the delete request is either 'ddd' indicating that only profiles for that specific daspace were to be deleted; MULTI indicating that profiles from multiple daspaces from the 'ddd' within the profile name through to the last profile for 'cachename' were to be deleted; or 'ALL', indicating that the _nnnnn profiles for all the daspaces for 'cachename' were to be deleted. *Error* is provided to assist IBM support personnel in identifying where in RACF the problem was discovered. RACF manager return and reason codes (in hexadecimal) are also provided.

If the problem was encountered while processing an R_cacheserv callable service invocation, another IRRL100xI message may also have been issued indicating the status of the cache being processed.

If the problem was encountered while processing an R_cacheserv callable service invocation and none of those messages were issued, or the request resulted from an RDELETE command, the status of the local cache is not affected by this problem.

Operator Response: Notify the System Programmer.

System Programmer Response:

- Look up the RACF manager return and reason codes on page "RACF Manager Return Codes" on page 307 to determine the cause of the problem.
- Contact your Security Administrator to check the status of the *cachename_ddd_nnnnn* profiles.

Security Administrator Response:

- Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS *cachename_ddd_nnnnn* profiles
- If scope is in the 'ddd' format and '_nnnnn' profiles remain for that particular 'ddd' and cachename whose name is equal to or greater than the profile named in the message, attempt to delete them with the RACF RDELETE command. If scope is 'MULTI' and any profiles remain for a daspace equal to or greater than the 'ddd' within the profile, attempt to delete them. If scope is 'ALL' and any '_ddd_nnnnn' profiles remain for that *cachename*, attempt to delete them all.
- If the problem persists, report the problem to the IBM Support Center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL1003I Cache is not affected. Error occurred while processing CACHECLS profile *profile-name*, error code = *error*, RACF manager return code = *retcode*, reason code = *rsncode*.

Explanation: An R_cacheserv callable service was invoked to retrieve the version level of the cache. During an attempt to read the specified profile to

IRRM001I • IRRM004I

determine if a the local cache had been hardened to the database, and if so retrieve its version level, an error occurred. Profile-name is in the format of either '*cachename*', or '*cachename_ddd_nnnnn*', where *cachename* is the value of the Cache_Name parameter on the R_Cacheserv callable service. '*ddd*' and '*nnnnn*' are the dataspace number and sequential number respectively (both in decimal) of one of the profiles holding the contents of that particular dataspace. *Error* is provided to assist IBM support personnel in identifying where in RACF the problem was discovered. RACF manager return and reason codes (in hexadecimal) are also provided to further delineate the problem.

The status of the local cache is not affected by this error: if the cache existed before the error it remains in existence. If a hardened version of the cache had existed on the RACF database as profiles in the CACHECLS class, this error results in an attempt to delete them.

System Action: RACF attempts to delete all the *cachename_ddd_nnnnn* profiles. If message IRRL1002I is not issued, the attempt was successful. If an IRRL1002I message is issued, then all

cachename_ddd_nnnnn profiles may not have been deleted.

Additionally, a symptom record for the error is created and stored in the LOGREC data set.

Operator Response: Notify the System Programmer.

System Programmer Response:

1. Look up the RACF manager return and reason codes in Chapter 9, "RACF return codes" on page 307 to determine the cause of the problem.
2. Contact your Security Administrator to check the status of the *cachename_ddd_nnnnn* profiles.

Security Administrator:

1. Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS *cachename_ddd_nnnnn* profiles.
2. If some remain, delete those profiles with the RACF RDELETE command.
3. If the problem persists, report the problem to the IBM support center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

TARGET command messages

IRRM001I *subsystem-name* **SUBSYSTEM TARGET COMMAND ENDED IN RECURSIVE ABEND.**

Explanation: The TARGET command abnormally ended in its attempt to recover from a prior abend on the indicated subsystem.

System Action: None.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM002I *subsystem-name* **SUBSYSTEM TARGET COMMAND HAS COMPLETED SUCCESSFULLY.**

Explanation: The TARGET command was processed by the *subsystem-name* subsystem without encountering any errors.

System Action: None.

Operator Response: None.

Destination: Descriptor code is 6.

IRRM003I *subsystem-name* **SUBSYSTEM TARGET COMMAND ENDED IN ERROR. [THE NODE WAS CREATED].**

Explanation: The TARGET command encountered an error during execution by the indicated subsystem. See any accompanying messages for more specific error information.

For new nodes, the node may or may not have been created. The message indicates when a node has been created.

System Action: None.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center if the accompanying error messages do not indicate user error.

Destination: Descriptor code is 6.

IRRM004I *subsystem-name* **SUBSYSTEM TARGET COMMAND WAS UNABLE TO OBTAIN STORAGE FOR NODE *node-name* SYSNAME *system-name*.**

Explanation: A new node, *node-name*, could not be defined by the TARGET command due to an unexpected storage shortage within the *subsystem-name* subsystem's address space.

System Action: The TARGET command ends in error.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Reissue the TARGET command to determine whether the storage shortage condition is persistent.

Problem Determination: If the storage shortage condition is persistent, obtain a dump of the *subsystem-name* subsystem's address space and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM005I *subsystem-name* **SUBSYSTEM TARGET COMMAND WAS UNABLE TO FIND DEFINITION OF NODE** *node-name* **[SYSNAME** *system-name*].

Explanation: The intended function could not be processed for node *node-name* because the node does not appear to have been defined by a previous TARGET command by the indicated subsystem.

System Action: The TARGET command ends in error.

Operator Response: This might indicate that an incorrect node name was specified on the command. Correct and reissue the command.

Destination: Descriptor code is 6.

IRRM006I *subsystem-name* **SUBSYSTEM TARGET COMMAND HAS FOUND THAT THE LOCAL NODE IS ALREADY DEFINED AS** *node-name*.

Explanation: An attempt to specify the LOCAL keyword for a node is disallowed. The TARGET command has found that a previous TARGET command by the indicated subsystem defined *node-name* to be the local node. Only one node may be designated as the local node.

System Action: The TARGET command ends in error.

Operator Response: If the failing TARGET command was issued during RACF parameter library processing, this may indicate a logical error within parameter library setup, such as the redundant or accidental inclusion of a given member. Report such an error to the system programmer. If the failing TARGET command was issued manually, TARGET LIST may be issued to display the defined nodes before proceeding with any subsequent TARGET command issuances.

System Programmer Response: If a logical error within the RACF parameter library setup is suspected, determine the set of members processed and their constituent commands. See *z/OS Security Server RACF Command Language Reference* for a description of the SET command and the SET INCLUDE() keyword and its implications for the order of command execution (if appropriate).

Destination: Descriptor code is 6.

IRRM007I *subsystem-name* **SUBSYSTEM TARGET COMMAND HAS FOUND THAT NODE(*) OR SYSNAME(*) CONFLICTS WITH ONE OR MORE SPECIFIED KEYWORDS.**

Explanation: NODE(*) is allowed only when the only function requested is a listing or SYSNAME(*), but one or more keywords other of the node definitions specifying the LIST keyword. When SYSNAME(*) is specified, the only other keywords allowed are NODE(*nodename*, DORMANT, OPERATIVE, DELETE, PURGE, or LIST. RACF detected a keyword other than the ones allowed.

System Action: The TARGET command is ignored.

Operator Response: Correct and reissue the command.

Destination: Descriptor code is 6.

IRRM008I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT DELETE LOCAL NODE** *node-name* **[SYSNAME** *system-name*] **WHILE OTHER NODES ARE DEFINED.**

Explanation: The TARGET command requires that the local node be the last TARGET definition deleted. Because this is not the case, the local node definition is not deleted. The TARGET command requires that the local member whose SYSNAME matches the CVTSNAME be the last TARGET definition deleted.

System Action: The TARGET command is ignored.

Operator Response: If the local node is a single-system node, first delete all remote nodes through appropriate TARGET commands. If the local node is a multisystem node, first delete all remote nodes and any member systems of the local node through appropriate TARGET commands, then reissue the command to delete the local node. Note that the local node and the operative remote nodes that are to be deleted must be made dormant prior to their deletion.

Destination: Descriptor code is 6.

IRRM009I **{LOCAL | REMOTE} RRSF NODE** *node-name* **[SYSNAME** *system-name*] **[(MAIN)] IS IN THE** *state* **STATE.**

Explanation: This is an informational message only. The state of the named node and system at the time of the invocation of the TARGET command is as given. If SYSNAME information is present in this message, the node *node-name* is a multisystem node. If MAIN is present in this message, the SYSNAME *system-name* is the receiver of the RRSF network traffic directed to this multisystem node.

IRRM010I • IRRM014I

Operator Response: None.

Destination: Descriptor code is 6.

IRRM010I *subsystem-name* **SUBSYSTEM
PROPERTIES OF {LOCAL | REMOTE}
RRSF NODE *node-name* [SYSNAME
system-name] [(MAIN)]:**

Explanation: This is an informational message only. This message precedes the remainder of the output displayed for node *node-name* by TARGET LIST processing. If SYSNAME information is present in this message, the node *node-name* is a multisystem node and the information is displayed for system *system-name* of the named node. If MAIN is present in this message, the SYSNAME *system-name* is the receiver of the RRSF network traffic directed to this multisystem node.

Operator Response: None.

Destination: Descriptor code is 6.

IRRM011I *subsystem-name* **SUBSYSTEM TARGET
COMMAND CANNOT MAKE NODE
node-name [SYSNAME *system-name*]
{OPERATIVE | DORMANT} BECAUSE
{ITS PROTOCOL IS UNKNOWN | ITS
LUNAME IS UNKNOWN | NO LOCAL
NODE OR SYSTEM IS DEFINED | ONE
OR MORE WORKSPACE FILES COULD
NOT BE ALLOCATED | A PREFIX
VALUE HAS NOT BEEN SPECIFIED |
NO LOCAL LUNAME IS DEFINED | NO
LOCAL MAIN IS DEFINED | NO
REMOTE MAIN IS DEFINED | THE
LOCAL NODE OR SYSTEM IS IN THE
INITIAL STATE}.**

Explanation: The state of node *node-name* is not changed for the reason given. If SYSNAME information is present in this message, the node *node-name* refers to a multisystem node and sysname *system-name* is a member system of that node.

Operator Response: Issue TARGET commands to provide the missing information along with the {OPERATIVE | DORMANT} keyword, as appropriate.

Destination: Descriptor code is 6.

IRRM012I **WARNING: SUBSYSTEM
subsystem-name IS OPERATING UNDER
A USERID THAT IS NOT PRIVILEGED
OR TRUSTED.**

Explanation: This message is generated only when the first RACF remote sharing TARGET command is issued and the user ID associated with the RACF address space is not privileged or trusted. IBM recommends that this user ID be privileged or trusted, but does not require it.

System Action: Processing continues.

System Programmer Response: The user ID associated with the RACF address space is not required to be privileged or trusted. However, if the user ID is not privileged or trusted, it must explicitly be given update access to all data sets used by RACF remote sharing facility (RRSF). Failure to do so results in access errors.

The user ID can be made privileged or trusted by activating the STARTED class and defining a profile for the user ID and specifying either privileged or trusted. The RACF address space must then be stopped and restarted. Alternatively, an entry for the user ID specifying either privileged or trusted can be made in the RACF started procedures table. However, the new entry does not take effect until the next IPL.

Destination: Descriptor code is 6.

IRRM013I *subsystem-name* **SUBSYSTEM TARGET
COMMAND HAS FOUND THAT THE
PREFIX SPECIFIED FOR NODE
node-name [SYSNAME *system-name*]
EXCEEDS THE MAXIMUM LENGTH OF
number CHARACTERS.**

Explanation: Prefix strings cannot exceed *number* characters due to workspace file naming conventions. The TARGET command has detected that the specified prefix exceeds this limit and does not update the prefix of node *node-name*. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Correct and reissue the command.

System Programmer Response: See *z/OS Security Server RACF System Programmer's Guide* for information on workspace file naming conventions.

Destination: Descriptor code is 6.

IRRM014I *subsystem-name* **SUBSYSTEM TARGET
COMMAND CANNOT CHANGE THE
PREFIX VALUE FOR NODE *node-name*
[SYSNAME *system-name*] BECAUSE
ITS WORKSPACE FILES ARE
ALREADY ALLOCATED.**

Explanation: The TARGET command has detected that one or more workspace data sets for node *node-name* are currently allocated and does not update the prefix of node *node-name*. A node's prefix is used in the formation of workspace file names and is changeable until those files have been allocated, which normally occurs during processing of a DORMANT/OPERATIVE keyword. After the files have been allocated, it cannot be changed. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Issue the TARGET NODE(*node-name*) LIST command to view information for node *node-name*, including its prefix. If a different prefix for node *node-name* is required, delete the node and redefine it with the new prefix. Note that a new prefix value causes a new set of workspace data sets to be created for the node after it is reactivated. See *z/OS Security Server RACF Command Language Reference* for information on the TARGET command and the disposition of workspace data sets affected by DELETE keyword processing.

Destination: Descriptor code is 6.

IRRM015I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT CHANGE THE WORKSPACE FILE ATTRIBUTES FOR NODE *node-name* [SYSNAME *system-name*] BECAUSE THE FILES ARE ALREADY ALLOCATED.**

Explanation: The TARGET command has detected that one or more workspace data sets for node *node-name* are currently allocated and does not update the workspace data set attributes for node *node-name*. A node's workspace file attributes are changeable until the files have been allocated, which normally occurs during processing of a DORMANT/OPERATIVE keyword. After the files have been allocated, the file attributes may not be changed. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Issue the TARGET NODE(*node-name*) LIST command to view information for node *node-name*, including its workspace file attributes. If different file attributes for node *node-name* are required, delete the node and redefine it with the new attributes. Note that new attributes might cause a new set of workspace files to be created for the node once it is reactivated. See *z/OS Security Server RACF Command Language Reference* for information on the TARGET command and the disposition of workspace data sets affected by DELETE keyword processing.

Destination: Descriptor code is 6.

IRRM016I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT CHANGE THE PROTOCOL INFORMATION FOR NODE *nodename* [SYSNAME *system-name*] WHILE IT IS OPERATIVE.**

Explanation: The TARGET command has detected an attempt to change the protocol information for a node that is in an operative state. A node's protocol information is changeable only if the node is in the dormant state, with the exception of LU name which can only be modified while the node is in the INITIAL state.

If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Issue the TARGET LIST command to view a summary of the nodes and their current states. If the protocol information for node *node-name* must be changed, issue the TARGET NODE(*node-name*) DORMANT command to change the state and allow a reissuance of the failed TARGET command to succeed. The reissued command may include the OPERATIVE keyword or a subsequent TARGET NODE(*node-name*) OPERATIVE command may be issued to reactivate the node when appropriate.

Destination: Descriptor code is 6.

IRRM017I *subsystem-name* **SUBSYSTEM TARGET COMMAND HAS DETERMINED THAT THE LUNAME *luname* IS ALREADY BEING USED BY NODE *node-name* [SYSNAME *system-name*].**

Explanation: Each node using the APPC protocol must have its own unique LU name. The TARGET command has detected an attempt to use an APPC LU name that is currently associated with another node. The LU name information for node *node-name* is not altered. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Correct and reissue the command. The TARGET NODE(*) LIST command may be issued to view information for each of the nodes, including their associated LU names.

Destination: Descriptor code is 6.

IRRM018I *subsystem-name* **SUBSYSTEM TARGET COMMAND HAS DETECTED A CONFLICT IN THE WORKSPACE FILE ATTRIBUTES FOR NODE *node-name* [SYSNAME *system-name*].**

Explanation: Volume specification and the specification of SMS information is not permitted on the same TARGET command. The current volume specification or SMS information for node *node-name* is not altered. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Issue the TARGET NODE(*node-name*) LIST command to view information for node *node-name*, including its volume specification or SMS information. Correct and reissue the command. Specifying VOLUME() causes any existing SMS information to be deleted. Similarly, specification of any of STORCLAS/MGMTCLAS/DATACLAS causes any existing volume specification to be deleted.

IRRM019I • IRRM023I

Destination: Descriptor code is 6.

IRRM019I *subsystem-name* **SUBSYSTEM TARGET COMMAND COULD NOT LOCATE VOLUME** *volume*. **UCBLOOK RETURN CODE IS** *return-code*. **UCBLOOK REASON CODE IS** *reason-code*.

Explanation: The TARGET command's attempt to locate a UCB for volume *volume* failed. No changes are made to the node's volume specification or SMS information.

System Action: The TARGET command ends in error.

Operator Response: Consult the *z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO* for the UCBLOOK service return and reason codes to determine why volume *volume* could not be located and take the appropriate action. Reissue a corrected version of the command, if necessary.

Destination: Descriptor code is 6. Routing code is 2.

IRRM020I *subsystem-name* **SUBSYSTEM PURGE OF NODE** *node-name* [**SYSNAME** *system-name*] **{INMSG | OUTMSG} FILE** *file-name* **ENDED IN ERROR.**

Explanation: The TARGET command was unable to erase all records from the INMSG or OUTMSG workspace file of node *node-name*. If the named node is a multisystem node, the member system's SYSNAME is displayed in the message.

System Action: The TARGET command ends in error.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: The error reflects a nonzero return code from a VSAM operation against the named workspace file.

If the integrity of the file is suspect, it might be necessary to replace the file. This can be done by deleting the node, erasing or renaming suspect file *file-name*, and then redefining the node. Alternatively, you could delete the node, then redefine it with a changed prefix to arrive at file names which differ from those of the previous workspace data sets.

If the integrity of the file is not suspect, the TARGET NODE(*node-name*) LIST command may be issued to determine the number of records in the file and a reissuance of the failed TARGET command can be attempted, if appropriate.

Destination: Descriptor code is 6.

IRRM021I *subsystem-name* **SUBSYSTEM PURGE OF NODE** *node-name* [**SYSNAME** *sysname*] **{INMSG | OUTMSG} FILE** *file-name* **IS COMPLETE.**

Explanation: The TARGET command has erased all records from the named file. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

Note: Commands pending to the file before its purge are processed.

System Action: The TARGET command ends successfully.

Operator Response: None.

Destination: Descriptor code is 6.

IRRM022I **RRSF NODE** *node-name* [**SYSNAME** *system-name*] **CANNOT BE DELETED BECAUSE IT IS IN THE** *state* **STATE.**

Explanation: An RRSF node cannot be deleted before it has first been made dormant. The indicated node was not deleted. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: To view a summary of the nodes and their current states, issue the TARGET LIST command. To delete node *node-name*, issue the TARGET NODE(*node-name*) DORMANT command, and then issue the TARGET LIST command to verify that node *node-name* is in a dormant state. Then reissue the failed TARGET NODE(*node-name*) DELETE command.

Destination: Descriptor code is 6.

IRRM023I **INTERNAL STATE TRANSITION ERROR DETECTED. RRSF NODE** *node-name* [**SYSNAME** *system-name*] **IS CURRENTLY IN THE** *state* **STATE.**

Explanation: Processing of the OPERATIVE/DORMANT/DELETE keyword of the TARGET command could not be completed successfully. The indicated RRSF node is left in the indicated connection state. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Report the occurrence of this message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM024I *subsystem-name* **SUBSYSTEM TARGET
COMMAND HAS FOUND THAT NO
NODES ARE CURRENTLY DEFINED.**

Explanation: No other information can be displayed in response to a TARGET LIST command because no nodes are defined.

System Action: The TARGET command ends successfully.

Operator Response: None.

Destination: Descriptor code is 6.

IRRM025I *subsystem-name* **SUBSYSTEM TARGET
COMMAND DOES NOT ALLOW THE
FILESIZE KEYWORD TO BE SPECIFIED
WITH A VALUE OF** *filesize*.

Explanation: The allowable range of values that can be specified with the FILESIZE keyword is 1 and 2147483647 (2 gigabytes minus 1).

System Action: The TARGET command ends in error.

Operator Response: Change the FILESIZE value and reissue the command. See *z/OS Security Server RACF System Programmer's Guide* for additional information.

Destination: Descriptor code is 6.

IRRM026I **NODE(*) AND SYSNAME(*) SHOULD
NOT BE SPECIFIED TOGETHER.
SYSNAME WILL BE IGNORED.**

Explanation: When NODE(*) is specified, the SYSNAME(*) keyword is not necessary and is ignored.

System Action: SYSNAME(*) is ignored and a detailed LIST of every node and sysname definition is displayed.

Operator Response: None.

Destination: Descriptor code is 6.

IRRM027I **RRSF NODE** *node-name* **IS A
MULTISYSTEM NODE AND THE
TARGET COMMAND MUST BE
SPECIFIED WITH A SYSNAME FOR
ALL FUNCTIONS EXCEPT LIST.**

Explanation: The SYSNAME() keyword is mandatory on all TARGET commands that refer to multisystem nodes, except for LIST. The SYSNAME() keyword was specified on a previous TARGET command for node *node-name*. When the keyword SYSNAME() is specified, the node is always considered a multisystem node.

System Action: The TARGET command is not processed.

Operator Response: Reissue the command with SYSNAME information or with SYSNAME(*) to display

all the systems associated with the specified node.

Destination: Descriptor code is 6.

IRRM028I **RRSF NODE** *node-name* **IS A
SINGLE-SYSTEM NODE AND MAIN
SHOULD NOT BE SPECIFIED.**

Explanation: Keyword MAIN can only be specified when referring to TARGET definitions that describe multisystem nodes.

System Action: The TARGET command ends in error.

Operator Response: If the single-system node is to be changed into a multisystem node, the TARGET command must include the new SYSNAME and the node *node-name* must be in one of the dormant states. Correct and reissue the command.

Destination: Descriptor code is 6.

IRRM029I **RRSF NODE** *node-name* **IS A
SINGLE-SYSTEM NODE AND THE
SYSNAME PARAMETER IS NOT
ALLOWED.**

Explanation: The keyword SYSNAME was specified on a TARGET command that refers to an already existing TARGET definition describing a single-system node. Because the node is already considered a single-system node, SYSNAME should not be specified.

System Action: The TARGET command is ignored.

Operator Response: If the single-system node is to be changed into a multisystem node, the TARGET command must also include the keyword MAIN and the node *node-name* must be in one of the dormant states. Correct and reissue the command.

Destination: Descriptor code is 6.

IRRM030I **RRSF NODE** *node-name* **[SYSNAME
system-name] MUST BE IN SOME
FORM OF THE DORMANT OR INITIAL
STATE TO REDEFINE A
SINGLE-SYSTEM NODE AS A
MULTISYSTEM NODE.**

Explanation: The keywords SYSNAME and MAIN were specified on a TARGET command that refers to an already existing TARGET definition describing a single-system node. Because SYSNAME and MAIN were specified on the TARGET command, RACF assumes that the single-system node is being redefined to be a multisystem node. This message is issued if either of the following occurs:

- You are redefining a remote single-system node to be a multisystem node, and the node is not in either the dormant or initial state.

IRRM031I • IRRM035I

- You are redefining a local single-system node to be a multisystem node, and one of its remote nodes is in a state other than the dormant or initial state.

System Action: The TARGET command is ignored.

Operator Response: If the single-system node is to be changed into a multisystem node, node *node-name* must be in the dormant or initial state. Reissue a corrected version of the command.

Destination: Descriptor code is 6.

IRRM031I **DEFINED RRSF NODE *node-name* SYSNAME *system-name* REQUIRES A PREFIX AND LUNAME TO CONFIGURE A NEW MAIN.**

Explanation: A TARGET command with keyword MAIN was issued to reconfigure the local system as the new MAIN system. RACF needs to access the workspace data sets used by the old MAIN system. In this case, RACF has looked for the PREFIX and LUNAME value that was specified on the TARGET statement for NODE *node-name* SYSNAME *system-name* and determined that one or both are missing. Because RACF cannot access the old MAIN's workspace data sets, the multisystem node is not reconfigured.

System Action: The TARGET command ends in error and a new MAIN is not configured.

Operator Response: Issue a TARGET command to supply node *node-name* sysname *system-name* with the missing information. Next, reissue the TARGET command to configure a new MAIN.

Destination: Descriptor code is 6.

IRRM032I *subsystem-name* **SUBSYSTEM TARGET COMMAND DOES NOT ALLOW NODE(*) AND SYSNAME TO BE SPECIFIED TOGETHER.**

Explanation: When specifying NODE(*) to perform the LIST function, a specific SYSNAME cannot be specified.

System Action: The TARGET command is ignored.

Operator Response: Reissue the correct version of the command, if necessary. You can enter NODE(*) SYSNAME(*) or NODE(*node-name*) SYSNAME(*system-name*).

Destination: Descriptor code is 6.

IRRM033I *subsystem-name* **SUBSYSTEM COULD NOT UPDATE STATUS OF NODE *node-name* SYSNAME *system-name* TO DEFINED.**

Explanation: In an attempt to update the status of node *node-name* system *system-name* to DEFINED, a resource lock could not be obtained.

System Action: The status of node *node-name* system *system-name* is not updated to DEFINED.

Operator Response: Reissue the same command. If the problem still exists, report the problem to the system programmer.

System Programmer Response: Gather the appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM034I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT CHANGE LUNAME BECAUSE RRSF NODE *node-name* [SYSNAME *system-name*] IS IN THE DORMANT STATE.**

Explanation: LU name cannot be modified when RRSF node *node-name* is in the DORMANT state. Local and remote LUNAMES are used for the workspace data set names. Records are queued in the workspace data sets when a node is DORMANT. Because of this, the workspace data set names cannot be changed when a node is DORMANT. If SYSNAME information is present in this message, the node *node-name* is a multisystem RRSF node.

System Action: The TARGET command ends in error.

Operator Response: Issue a TARGET DELETE command to delete the node. Then issue a TARGET command to redefine it with the new LU name. Update the RACF parameter library if necessary.

Destination: Descriptor code is 6.

IRRM035I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT MAKE NODE *node-name* SYSNAME *system-name* {DORMANT | OPERATIVE} BECAUSE ONLY THE DEFINED STATE IS ALLOWED.**

Explanation: The keyword OPERATIVE or DORMANT was specified on the TARGET command and because of the current configuration, node *node-name* system *system-name* can only be in the DEFINED state. This message is written to the SYSLOG.

System Action: The OPERATIVE or DORMANT keyword is ignored and the TARGET command continues processing the remaining keywords.

Operator Response: None.

IRRM036I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT DELETE NODE**
node-name **MAIN SYSTEM** *system-name*
BECAUSE OTHER SYSTEMS EXIST IN
NODE *node-name*.

Explanation: The TARGET command has detected an attempt to delete the MAIN system *system-name* of multisystem node *node-name* before all non-MAIN systems of node *node-name* have been deleted. TARGET command requires that the MAIN system be the last system deleted from a remote multisystem node.

System Action: The TARGET command ends in error and the TARGET definition for node *node-name* system *system-name* is not deleted.

Operator Response: Issue the appropriate TARGET commands to delete all non-MAIN systems of the multisystem node first, then reissue the original TARGET command to delete the MAIN system.

Destination: Descriptor code is 6.

IRRM037I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT ALLOCATE**
WORKSPACE DATASETS FOR NODE
node-name **SYSNAME** *system-name*.

Explanation: A TARGET command attempted to change the system of a multisystem node that is considered the MAIN system. When this message is issued, the TARGET command either did not attempt to allocate the {INMSG | OUTMSG} workspace files of node *node-name* system *system-name* or it received a failure while attempting to allocate.

System Action: The TARGET command ends in error.

Operator Response: If allocation was not attempted, associated messages indicate the information that is needed. See the operator responses in each case. After supplying the information needed through additional TARGET commands, reissue the original command. If no other TARGET messages exist, allocation was attempted and failed. Report this failure to the system programmer.

System Programmer Response: Gather appropriate diagnostic information for the failing DYNALLOC and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM038I **RRSF NODE** *node-name* {**SYSNAME**
system-name} **MUST BE IN THE**
DORMANT STATE TO CONFIGURE A
NEW MAIN.

Explanation: While configuring a new MAIN system in a multisystem node, a TARGET command located a node definition that should have a status of DORMANT,

but it is in either the DEFINED, INITIAL, or one of the OPERATIVE states.

System Action: The TARGET command ends in error.

Operator Response: Issue the appropriate TARGET commands to put the named node and system in the DORMANT state. Reissue the original command to configure a new MAIN system.

Destination: Descriptor code is 6.

IRRM039I **RRSF NODE** *node-name* {**SYSNAME**
system-name} **MUST BE IN THE**
DEFINED OR DORMANT STATE TO
CONFIGURE A NEW MAIN.

Explanation: While configuring a new MAIN system in a multisystem node, a TARGET command located a node definition that should have a status of DEFINED or DORMANT, but it is in the INITIAL or one of the OPERATIVE states.

System Action: The TARGET command ends in error.

Operator Response: Issue the appropriate TARGET commands to put the named node and system in the DEFINED or DORMANT state. System definitions in a multisystem node may not be in the DEFINED state because a MAIN system for the multisystem node has not been defined. After issuing the appropriate TARGET commands, issue the original TARGET command to configure a new MAIN system.

Destination: Descriptor code is 6.

IRRM040I **RRSF NODE** *node-name* {**SYSNAME**
system-name} **MUST BE IN THE**
DEFINED STATE TO CONFIGURE A
NEW MAIN.

Explanation: While configuring a new MAIN system in a multisystem node, a TARGET command located a node definition that should have a status of DEFINED, but it is in the INITIAL state or one of the OPERATIVE or DORMANT states.

System Action: The TARGET command ends in error.

Operator Response: Issue the appropriate TARGET commands to put the named node and system in the DEFINED state. System definitions in a multisystem node might not be in the DEFINED state because a MAIN system for the multisystem node has not been defined. After issuing the appropriate TARGET commands, issue the original TARGET command to configure a new MAIN system.

Destination: Descriptor code is 6.

IRRM041I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT DELETE THE LOCAL NODE *node-name* MAIN SYSTEM *system-name* BECAUSE REMOTE RRSF NODES EXIST.**

Explanation: The local MAIN system cannot be deleted until all remote RRSF nodes are deleted.

System Action: The TARGET command ends in error.

Operator Response: Issue the appropriate TARGET commands to delete all remote RRSF nodes. Next, reissue the failed TARGET command.

Destination: Descriptor code is 6.

IRRM049I *subsystem-name* **SUBSYSTEM REQUIRES SMS STORCLAS SPECIFICATION IN ORDER TO ALLOCATE THE {INMSG | OUTMSG} WORKSPACE FILE OF NODE *node-name* [SYSNAME *system-name*].**

Explanation: An SMS allocation for a node's workspace data sets cannot be made without a STORCLAS specification. The TARGET command has detected the absence of such a specification for node *node-name* and does not attempt to allocate the node's workspace data sets. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Issue TARGET commands to provide the missing information along with the OPERATIVE or DORMANT keyword, as appropriate.

Destination: Descriptor code is 6.

IRRM050I *subsystem-name* **SUBSYSTEM REQUIRES VOLUME SPECIFICATION IN ORDER TO ALLOCATE THE {INMSG | OUTMSG} WORKSPACE FILE OF NODE *node-name* [SYSNAME *system-name*].**

Explanation: The absence of SMS information implies that a non-SMS allocation should be made for a node's workspace data sets. This, in turn, requires a volume specification. The TARGET command has detected the absence of such a specification for node *node-name* and does not attempt to allocate the node's workspace data sets. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Issue TARGET commands to provide the missing information along with the OPERATIVE or DORMANT keyword, as appropriate.

Destination: Descriptor code is 6.

IRRM052I *subsystem-name* **SUBSYSTEM WAS UNABLE TO ALLOCATE THE {INMSG | OUTMSG} WORKSPACE FILE OF NODE *node-name* [SYSNAME *system-name*].**

Explanation: The TARGET command either did not attempt to allocate the INMSG or OUTMSG workspace file of node *node-name* or it received a failure while attempting to allocate it. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: If allocation was not attempted, associated messages indicate the information whose absence prevented the attempt from being made. See the operator responses in each case. If no associated messages exist, allocation was attempted and failed. Report this failure to the system programmer.

System Programmer Response: Gather appropriate diagnostic information for the failing DYNALLOC and contact the IBM support center, if necessary.

Destination: Descriptor code is 6.

IRRM053I **THE {INMSG | OUTMSG} WORKSPACE DATA SET OF (*subsystem-name*) SUBSYSTEM IS NOT ALLOCATED FOR NODE (*node-name*). THE DATA SET CANNOT BE PURGED.**

Explanation: The TARGET command was unable to erase all records from the indicated data set of node *node-name* because no data set is allocated. This could be because

- the data set information was never provided by the user, or
- the RACF remote sharing facility (RRSF) marked the data set in error and deallocated it.

System Action: The TARGET command ends in error.

Operator Response: If this message occurred because the data set information was never provided by the user, issue the TARGET NODE(*node-name*) DORMANT command and supply any missing information. Refer to message IRRM011I for an indication of the missing information. Also, see *z/OS Security Server RACF Command Language Reference* for information on the TARGET command.

If this message occurred because the RACF remote sharing facility (RRSF) marked the data set in error and deallocated it, issue:

- The TARGET NODE(*node-name*) LIST command to find out if the data set is allocated by RRSF.
- The TARGET NODE(*node-name*) DORMANT command to cause RRSF to attempt to allocate the

data set. Next, issue the TARGET NODE(*node-name*) PURGE (INMSG/OUTMSG) command to purge the requested data set.

If you receive additional error messages indicating that the above commands did not work, use the standard data management commands to correct and update the data set.

Destination: Descriptor code is 6.

IRRM054I *subsystem-name* **SUBSYSTEM WAS UNABLE TO ALLOCATE OUTMSG WORKSPACE FILE** *workspace-dataset-name* **OF NODE** *node-name* **[SYSNAME** *system-name* **] FOR DEFINING OLD MAIN SYSNAME** *system-name*.

Explanation: While configuring a new MAIN system in a multisystem node, an error was encountered while attempting to allocate a workspace data set previously used by the old MAIN system of this local node, *node-name*. Shared DASD and a shared VSAM catalog is recommended for the RRSF workspace data sets due to this operation and when they are not used, the workspace data set must be manually copied from the old MAIN system to this new MAIN system (using the same workspace filename).

System Action: The TARGET command ends in error.

Operator Response: Manually copy the workspace data set from the old MAIN system to this new MAIN system (using the same workspace filename) so that this operation can continue.

Destination: Descriptor code is 6.

IRRM055I *subsystem-name* **SUBSYSTEM TARGET COMMAND CANNOT CHANGE THE WDSQUAL VALUE FOR NODE** *node-name* **[SYSNAME** *system-name* **] BECAUSE ITS WORKSPACE FILES ARE ALREADY ALLOCATED.**

Explanation: The TARGET command has detected that one or more workspace data sets for local node *node-name* are currently allocated and does not update the WDSQUAL of node *node-name*. A node's WDSQUAL is used in the formation of workspace data set names and is changeable until those data sets have been allocated, which normally occurs during processing of a DORMANT/OPERATIVE keyword. After the data sets have been allocated, it cannot be changed. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The TARGET command ends in error.

Operator Response: Issue the TARGET NODE(*node-name*) LIST command to view information for node *node-name*, including its WDSQUAL. If a different WDSQUAL for node *node-name* is required, delete the node and redefine it with the new

WDSQUAL. Note that a new WDSQUAL value causes a new set of workspace data sets to be created for the node once it is reactivated. See *z/OS Security Server RACF Command Language Reference* for information on the TARGET command and the disposition of workspace data sets affected by DELETE keyword processing.

Destination: Descriptor code is 6.

IRRM056I *subsystem-name* **SUBSYSTEM TARGET COMMAND SPECIFIED A WDSQUAL FOR NODE** *node-name* **[SYSNAME** *system-name* **] WHICH IS CURRENTLY NOT DEFINED AS A LOCAL NODE. THE VALUE IS ACCEPTED BUT WILL NOT BE USED UNTIL THE NODE IS DEFINED AS LOCAL.**

Explanation: The TARGET command has detected that a WDSQUAL was specified for a node that is not defined as a local node. WDSQUAL is only used in the formation of workspace data set names for nodes that are defined as local. Specifying WDSQUAL for a remote node causes the WDSQUAL to be ignored in the creation of its workspace data set names unless the node is defined as local in a subsequent TARGET command.

System Action: Processing continues.

Destination: Descriptor code is 6.

IRRM080I *subsystem-name* **SUBSYSTEM TARGET COMMAND ENCOUNTERED AN ERROR. ABEND CODE IS** *returncode-reasoncode*.

Explanation: The TARGET command processed by the *subsystem-name* subsystem ended abnormally, with the given return and reason codes.

Operator Response: Report the occurrence of this message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM082I *subsystem-name* **SUBSYSTEM TARGET COMMAND IS ALREADY PROCESSING.**

Explanation: The issuance of a TARGET command to be processed by the *subsystem-name* subsystem prior to the completion of a concurrent TARGET command has been detected. The processing of concurrent TARGET commands is not allowed.

System Action: The TARGET command is ignored.

Operator Response: The TARGET command may be reissued after the processing TARGET command has

IRRM083I • IRRM086I

signalled its completion with message IRRM002I or IRRM003I.

Problem Determination: None.

Destination: Descriptor code is 6.

IRRM083I **ISSUER HAS INSUFFICIENT AUTHORITY TO KEYWORD *keyword* ON *subsystem-name* SUBSYSTEM TARGET COMMAND.**

Explanation: RACF OPERCMDS class profiles currently fail to authorize the command issuer to use the named keyword with the TARGET command when invoking its execution by the *subsystem-name* subsystem.

System Action: The TARGET command is ignored.

Operator Response: See your RACF security administrator to obtain the proper authority.

Destination: Descriptor code is 6.

IRRM084I **THE *keyword* KEYWORD REQUIRES ADDITIONAL SPECIFICATION.**

Explanation: The *keyword* keyword requires the specification of 1 or more of its options.

System Action: The TARGET command is ignored.

Operator Response: Reissue a corrected version of the command, if necessary. For the syntax of the TARGET command, see *z/OS Security Server RACF Command Language Reference*.

Destination: Descriptor code is 6.

IRRM085I **NODE *node-name* {SYSNAME *system-name*} CANNOT BE PURGED BECAUSE IT IS NOT DORMANT.**

Explanation: A node's workspace data sets cannot be purged unless the node is dormant. The TARGET command has detected that node *node-name* is not dormant. If SYSNAME information is included in the message, node *node-name* is a multisystem node.

System Action: The TARGET command is ignored.

Operator Response: This may indicate that an incorrect node name was specified on the command. A TARGET NODE(*node-name*) LIST command can be issued to determine the state of node *node-name*. Issue a TARGET NODE(*node-name*) DORMANT command to make the node dormant, and then repeat the TARGET NODE(*node-name*) PURGE command.

Destination: Descriptor code is 6.

IRRM086I *subsystem-name* **SUBSYSTEM TARGET COMMAND REQUIRES THAT A NODE BE SPECIFIED.**

Explanation: The NODE() keyword must be specified on any TARGET command that has additional keywords. The TARGET command has detected the presence of one or more such keywords along with the absence of the NODE() keyword.

System Action: The TARGET command is ignored.

Operator Response: Reissue a corrected version of the command, if necessary.

Destination: Descriptor code is 6.

RRSF connection receive transaction program messages

IRRN000I RACF APPC RECEIVE TRANSACTION PROGRAM STARTING FOR LU *luname* NODE *node-name* [SYSNAME *system-name*].

Explanation: This is an informational message that is written to the SYSLOG after the program that receives APPC messages completes its initialization. The program now notifies APPC that it is ready to handle any messages from the indicated node. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

IRRN003I APPC RECEIVE TRANSACTION PROGRAM OPERATING UNDER USER ID *userid* GROUP *group-name*.

Explanation: This message is written to the SYSLOG after the program that receives APPC messages completes its initialization. The program now notifies APPC that it is ready to handle any messages from the indicated node. This is an informational message.

IRRN009I RACF APPC RECEIVE TRANSACTION PROGRAM COMPLETED FOR LU *luname* NODE *node-name* [SYSNAME *system-name*].

Explanation: This message is written to the SYSLOG after the program that receives APPC messages stops processing incoming messages. The program stops as a result of an operator request to make the node dormant or as the result of a operational error. Earlier messages might indicate the nature of the problem. If SYSNAME information is present in this message, the node *node-name* is a multisystem node.

System Action: The indicated node cannot send new work into the local node until the local node is returned to operative active status. Work requests active in the RACF subsystem address space for the indicated node continue to run. Any output directed to the failing node is held in the named node's OUTMSG workspace data set.

Operator Response: Review the console log for an indication of the original error.

IRRN020I APPC RECEIVE AND WAIT STARTING FOR LU *luname* NODE *node name* [SYSNAME *system-name*].

Explanation: This message is written to the SYSLOG immediately before the program notifies APPC that it will receive messages for the named LU name. If SYSNAME information is present in this message, the node *nodename* is a multisystem node.

System Action: RACF continues processing.

Problem Determination: Under normal circumstances, this message can be ignored. When diagnosing a problem with a particular node, this

message can be used with its companion messages to identify the part of the process that is failing.

When the receive program starts, it issues messages IRRN000I and IRRN003I. You can use these messages to verify that the correct APPC conversation was established and that it is established under the correct authority.

After issuing the messages, the program reads the INMSG workspace data set for any work that did not complete before the node became inactive.

Following the recovery of the held work requests, message IRRN020I is issued and APPC is notified. If IRRN009I appears, there is a problem in passing the work requests onto the task that routes the work within the subsystem address space.

IRRN021I APPC RECEIVE AND WAIT ENDING FOR LU *luname* NODE *node-name* [SYSNAME *system-name*].

Explanation: This message is written to the SYSLOG when the program that receives APPC messages begins its shutdown. The program notified APPC that it will not handle any messages from the indicated node. If SYSNAME information is present in this message, the indicated node *node-name* is a multisystem node. This is an informational message.

System Action: Any work requests for the indicated node continues to run, but any output to the remote node is held in the OUTMSG workspace data set until the node becomes operative.

Problem Determination: This message should follow an operator command making the node dormant or follow a failure message. Refer to the failure message for corrective actions.

IRRN080I *subsystem-name* RACF SUBSYSTEM APPC RECEIVE TRANSACTION PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS *abend-code*.

Explanation: Every RACF remote sharing system has a APPC receive program receiving messages from other nodes defined to RACF. The receive transaction program had an error. This message appears every time an abnormal event occurs. This message is written to the SYSLOG.

System Action: The transaction program attempts to retry during its startup processing when it is starting work from the INMSG workspace data set. If an abend occurs during this processing, the program discards the record and reads the next record in the data set. When all records have been read, the subsystem notifies APPC that it is ready to receive new messages.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work

IRRN081I • IRRO081I

in its input queue. For a complete discussion, see *z/OS Security Server RACF Diagnosis Guide*.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

IRRN081I *subsystem-name* **RACF SUBSYSTEM
APPC RECEIVE TRANSACTION
PROGRAM ENCOUNTERED AN
ERROR. ABEND CODE IS *abend-code*.
RECEIVE TRANSACTION PROGRAM
ENDING.**

Explanation: Every RACF remote sharing system has a APPC receive program receiving messages from other nodes defined to RACF. The receive transaction program had an error.

System Action: The transaction program cannot retry from this abnormal error. The program releases all system resources it holds and ends processing. The node connection program attempts to restart the receive transaction program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see *z/OS Security Server RACF Diagnosis Guide*.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

Destination: Descriptor code is 6. Routing code is 2.

RRSF connection send transaction program messages

IRRO080I *subsystem-name* **RACF SUBSYSTEM
APPC SEND TRANSACTION
PROGRAM ENCOUNTERED AN
ERROR. ABEND CODE IS *abend-code*.**

Explanation: Every RACF remote sharing system has a APPC send program sending messages to other nodes defined to RACF. The send transaction program had an error. This message appears every time an abnormal event occurs. This message is written to the SYSLOG.

System Action: The transaction program attempts to retry the current transaction.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see *z/OS Security Server RACF Diagnosis Guide*.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

nodes defined to RACF. The send transaction program had an error. This message appears every time an abnormal event occurs.

System Action: The transaction program cannot retry from this abnormal error. The program releases all system resources it holds and ends processing. The node connection program attempts to restart the send transaction program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see *z/OS Security Server RACF Diagnosis Guide*.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

Destination: Descriptor code is 6. Routing code is 2.

IRRO081I *subsystem-name* **RACF SUBSYSTEM
APPC SEND TRANSACTION
PROGRAM ENCOUNTERED AN
ERROR. ABEND CODE IS *abend-code*.
SEND TRANSACTION PROGRAM
ENDING.**

Explanation: Every RACF remote sharing system has a APPC send program sending messages to other

RRSF (RACF remote sharing facility) general messages

IRRP003I *subsystem-name* **SUBSYSTEM WAS UNABLE TO ISSUE IEFSSREQ REQUEST. RETURN CODE IS: *return-code*.**

Explanation: An attempt to send a request to the MVS IEFSSREQ subsystem has failed. Profiles have been updated on the source-node.

System Action: IEFSSREQ request processing ends.

Operator Response: Report this message to your system programmer.

System Programmer Response: The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

Return Code	Function
4	The subsystem does not support this function.
8	The subsystem exists, but is not active.
12	The subsystem is not defined in the IEFSSNxx parmlib member.
16	The function has not completed. This is a disastrous error.
20	The SSOB or SSIB have invalid lengths or formats.
24	The SSI has not been initialized.

A return code of 4, 16, 20, or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See *z/OS Security Server RACF Migration* for installation considerations and *z/OS Security Server RACF System Programmer's Guide* for configuration considerations for the RACF subsystem.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRP004I *subsystem-name* **SUBSYSTEM IEFSSREQ REQUEST ENDED WITH A RETURN CODE OF *return-code*.**

Explanation: An attempt to send a request to the MVS IEFSSREQ subsystem interface failed. No profiles have been updated.

System Action: RACLINK command processing ends.

Operator Response: Report this message to your system programmer.

System Programmer Response: The return code indicated in this message is the value of the SSOBRETN field in the subsystem's option block

(SSOB). The return code may be one of these values:

Code	Explanation
8	The subsystem could not execute the command because of an internal parameter error, or the subsystem supports this request, but is not active.
16	The caller is not APF-authorized, or storage is not available for an internal data area.

Contact the IBM support center to report this problem.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRP010I **RACF ICHEINTY RC *return-code* RECEIVED WHILE {DEFINING | APPROVING | DELETING | RETRIEVING} ASSOCIATION (*node-name.userid*) FOR USER *target-userid*.**

Explanation: The association information for the *target-userid* could not be defined, approved, deleted or retrieved due to an unexpected RACF error condition.

System Action: RACLINK command ends processing.

User Response: Contact your RACF administrator to examine the supplied return code.

RACF Security Administrator Response: Analyze the supplied return code by reading the return code description for the ICHEINTY macro in *z/OS Security Server RACF Macros and Interfaces*. Contact the IBM support center, if necessary.

Destination: Descriptor code is 6. Routing code is 9.

IRRP015I **NODE *node-name* SPECIFIED FOR AUTOMATIC DIRECTION PROCESSING IS NOT CORRECT.**

Explanation: The RACF subsystem address space attempted to send command output or results from one of the following to the indicated node:

- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

The node name was specified on a previous SET command in either the OUTPUT or NOTIFY operand and is not correct.

System Action: The command output or results are not returned to the intended node.

User Response: Issue the SET LIST command to display the current OUTPUT and NOTIFY settings. Note where the incorrect node name appears. If the node name is in error, issue the SET command with the

IRRP016I • IRRP021I

appropriate OUTPUT and NOTIFY keywords to correct the error. If the node name is valid, issue a TARGET command to define the node.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRP016I **Undefined association**
(*node-name.userid*) could not be
{deleted | retrieved} by userid *userid* at
node *node-name*.

Explanation: The RACLINK APPROVE or RACLINK UNDEFINE command failed because the user ID association does not exist on the target side. The user ID association has been updated on the source user ID, but not on the target user ID. This message is sent to the TSO terminal of the RACLINK issuer or the target user.

System Action: RACLINK command ends processing.

User Response: If you issued the failing RACLINK APPROVE command, you need to use the RACLINK UNDEFINE(*node-name.userid*) command to delete any indicators of a user ID association between you and *node-name.userid*. Then use the RACLINK DEFINE(*node-name.userid/password*) command or both RACLINK DEFINE(*node-name.userid*) command on this node and RACLINK APPROVE command on node *node-name* to complete the definition of the user ID association.

IRRP017I **The requested association could not**
be {defined | approved | deleted |
retrieved | updated} because user
***userid* is not RACF defined.**

Explanation: The association specified on the RACLINK LIST, DEFINE, APPROVE or UNDEFINE command could not be located because the target user ID is not defined to RACF. The source user ID may have been updated. This message is sent to the TSO terminal of the RACLINK issuer or the target user.

System Action: RACLINK command processing completes.

User Response: Either add the target user ID via the ADDUSER command or contact your RACF administrator to do so. After the problem has been corrected, try the command again.

IRRP018I **An existing association was found for**
user *userid* on target node *node-name*.

Explanation: A RACLINK DEFINE was issued for an association that already exists on the target node. The source user ID was updated, but the target user ID was not. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: RACLINK command processing completes.

User Response: Issue the RACLINK DELETE command to delete the existing association and then try the command again.

IRRP019I **Association key length *length* is not**
valid. Information cannot be retrieved
for user *userid*.

Explanation: A RACLINK command has failed because the user ID and node are too long. This error is due to an internal problem. This message is sent to the RACLINK issuer.

System Action: RACLINK command processing ends. No RACLINK association is retrieved.

User Response: Contact IBM support to correct the faulty key length.

IRRP020I **RACF ICHEINTY rc *return-code* received**
while {defining | approving | deleting |
retrieving | updating} association
(*node-name.userid*) for user *userid*.

Explanation: The RACLINK command failed while attempting to define, approve, delete, retrieve, or update the association information for the specified user ID. This may have occurred on the local node or a different node. This message is sent to the TSO terminal of the RACLINK issuer or the target user.

System Action: RACLINK command ends processing. No RACLINK association is retrieved.

User Response: Contact your system programmer to analyze the supplied return codes.

System Programmer Response: To determine the meaning of these ICHEINTY return codes, see *z/OS Security Server RACF Macros and Interfaces*.

IRRP021I **RACLINK could not be completed**
because target node *node-name* is
undefined.

Explanation: RACF is unable to locate the node name specified. This message is sent to the TSO terminal of the target user.

System Action: RACLINK command ends processing. A RACLINK association on the source user ID may have been updated.

User Response: Verify that this is a legitimate node to be sending commands to and, if it is, contact your system programmer to have the remote node defined to RACF.

System Programmer Response: Issue the TARGET LIST command to determine the status of the target node. Use the TARGET command if the node needs to be defined.

IRRP022I RACLINK command was unable to obtain storage for the association entry.

Explanation: A failure occurred while attempting to obtain storage necessary to update an association entry in the target user's profile. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: RACLINK command processing ends. The local user profile has been updated, but the target user profile has not been updated.

User Response: Notify the system programmer. Once the storage problem has been resolved, delete the association from the local user profile and issue the failing RACLINK command again.

System Programmer Response: Note the message number and any other diagnostic information generated, and contact your IBM support center.

Problem Determination: The storage request was for subpool 1.

IRRP080I subsystem-name SUBSYSTEM MESSAGE TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

Explanation: The MESSAGE handler task was processing a command or returned output. This message appears when an abnormal event occurs.

System Action: The MESSAGE handler attempts to retry the current work request. If the retry does not work, message IRRP081I is issued.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

Destination: Descriptor code is 1. Routing codes are 2 and 9.

IRRP081I subsystem-name SUBSYSTEM MESSAGE TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. MESSAGE HANDLING TASK ENDING.

Explanation: The message handler subtask was processing a command or returned output. This message appears when an abnormal event occurs.

System Action: The message handler subtask ends and the parent task attempts to restart the message handler subtask.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*. The task that

started the message handler task attempts to restart the task. Verify that message IRRB020I was issued showing that the task restart was successful.

Destination: Descriptor code is 6. Routing code is 2.

IRRP092I {Peer | Managed} association with target-userid at node node-name established for you by user ID userid.

Explanation: An association with *target-userid* has been established for you by *userid*. This message is sent to the TSO terminal of the target user.

System Action: The RACLINK command completes successfully.

User Response: None.

IRRP093I {Peer | Managed} association with userid at node-name issued by command-issuer pending due to an {expired | incorrect} password.

Explanation: A RACLINK DEFINE command was issued by *command-issuer* to associate your user ID with *userid*. The association is pending approval since the password provided was expired or incorrect. This message is sent to the TSO terminal of the RACLINK issuer or the target user.

System Action: The RACLINK command processing completes. The association is pending approval.

User Response: If the association is desired, you can approve the association with the RACLINK APPROVE command.

IRRP094I {Peer | Managed} association with userid at node node-name issued by command-issuer waiting for your approval.

Explanation: A RACLINK DEFINE specifying you as the target user ID was issued by the *command-issuer*. The association is not active until you approve it. This message is sent to the TSO terminal of the target user.

System Action: The RACLINK command has completed processing. The association is pending approval.

User Response: If the association is desired, approve the association with the RACLINK APPROVE command.

IRRP095I {Peer | Managed} association with userid1 at node-name by userid2 failed because user access has been revoked.

Explanation: The indicated association for *userid2* could not be defined because *userid1*'s access has been revoked. This message is sent to the TSO terminal of the RACLINK issuer.

IRRP096I • IRRP109I

System Action: The RACLINK command stops processing.

User Response: Contact your RACF security administrator to find out why *userid1* has been revoked, and to possibly have it resumed.

IRRP096I {Peer | Managed} association with *userid* at node *node-name* by *command-issuer* failed. RACROUTE VERIFY RACF rc is *return-code*.

Explanation: A RACLINK DEFINE command was issued and the validity checking for the remote user ID failed. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: The RACLINK command stops processing.

User Response: To determine the exact cause of the failure, see the information on RACROUTE REQUEST=VERIFY in *z/OS Security Server RACROUTE Macro Reference*.

IRRP097I {Peer | Managed} association with *userid* at node *node-name* has been approved.

Explanation: The indicated association has been approved. Remote sharing requests to the target user ID are processed. This message is sent to the TSO terminal of the RACLINK issuer or the target user.

System Action: The RACLINK command completes processing.

User Response: None.

IRRP104I Association (*node-name.userid*) has been deleted by *userid* at node *node-name*.

Explanation: The specified association has been deleted from your user ID profile by the specified user ID. This message is sent to the TSO terminal of the target user.

System Action: The RACLINK command completes processing.

User Response: None.

IRRP107I A duplicate approval received and ignored from *userid* *userid* at node *node-name*

Explanation: Either a RACLINK DEFINE or a RACLINK APPROVE command was issued specifying

your user ID as the target of the command. However, this user ID association is already created and approved in your user ID profile. No update has been made to your user ID profile. This message is sent to the TSO terminal of the target user.

System Action: The RACLINK command ends.

User Response: None.

IRRP108I RACLINK issued at *node-name* to associate you with *userid* has failed. Entry already exists.

Explanation: The RACLINK entry could not be defined because of a mismatch. This could have occurred because:

- The association already exists in your user ID profile, but the association is waiting for approval from *userid*.
- The association already exists in your user ID profile, but the association type is different. For example, the existing association is of type PEER and an attempt was made to create of association of type MANAGED.

This message is sent to the TSO terminal of the target user.

System Action: The RACLINK command ends processing. A pending association has been created in the source user ID profile, and the association in the target user ID profile remains unchanged.

User Response: If the association needs to be modified, delete it using the UNDEFINE operand of the RACLINK command. Follow this by issuing a RACLINK DEFINE command.

IRRP109I RACLINK from user ID *userid* to associate your user ID with *node-name.userid* is pending.

Explanation: The user ID association is pending approval from the specified user ID. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: The RACLINK command processing completes. The user ID association is pending approval by the indicated user ID.

User Response: Wait until the user ID association is approved by the approving user ID, or contact the owner of the approving user ID to request approval of the user ID association.

Problem Determination: For information on the pending association waiting for your approval, use the RACLINK LIST command.

RRSF connection task messages

IRRQ015I *task-name* **TASK IN** *subsystem-name*
SUBSYSTEM HAS ENDED
ABNORMALLY.

Explanation: During the shutdown process, the task *task-name* in the subsystem *subsystem-name* would not voluntarily shut down. The CONNECTION program has waited a sufficient interval for the task to end, without success. The task is forcibly ended. This message is written to the SYSLOG.

System Action: Task *task-name* is ended abnormally. The CONNECTION program continues the shutdown process.

Operator Response: Report the exact text of this message to your system programmer.

System Programmer Response: Examine any system dumps obtained.

IRRQ080I *subsystem-name* **SUBSYSTEM APPC**
CONNECTION TASK HAS
ENCOUNTERED AN ERROR. ABEND
CODE IS *abend-code*.

Explanation: The CONNECTION task was changing the status of an APPC conversation and the related transaction programs because of a TARGET command request. This message appears when an abnormal event occurs. This message is written to the SYSLOG.

System Action: The CONNECTION task attempts to retry the current status change request.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see *z/OS*

Security Server RACF Diagnosis Guide.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

IRRQ081I *subsystem-name* **SUBSYSTEM APPC**
CONNECTION TASK HAS
ENCOUNTERED AN ERROR. ABEND
CODE IS *abend-code*. **CONNECTION**
TASK ENDING.

Explanation: The CONNECTION task was changing the status of an APPC conversation and the related transaction programs because of a TARGET command request. This message appears when an abnormal event occurs during a task you cannot retry.

System Action: The CONNECTION task releases system resources it holds and ends processing.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see *z/OS Security Server RACF Diagnosis Guide*.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*. The task that started the CONNECTION task attempts to restart the task. Verify that message IRRB020I was issued showing that the task restart was successful.

Destination: Descriptor code is 6. Routing code is 2.

RRSF output handling task messages

IRRR001I **RACF command output transmitted**
because user data set *data-set-name* **is**
full.

Explanation: Output was returned from one of the following to the issuer via TSO TRANSMIT because the user's output data set is full:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

This message is sent to the user's TSO terminal.

System Action: None.

User Response: Allocate a larger data set or delete lines from the existing data set.

IRRR002I **RACF command output transmitted**
because user data set *data-set-name* **could not be allocated. Allocation**
return code was *return-code*.

Explanation: Output was returned from one of the following to the issuer via TSO TRANSMIT because allocation of the user's output data set failed with the indicated return code.

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

During returned output processing, RACF performs dynamic allocation for the RRSFLIST data set. If this fails, RACF returns the return code. This message is sent to the user's TSO terminal.

IRRR003I • IRRR007I

System Action: None.

User Response: Report the complete text of this message to the system programmer.

System Programmer Response: The MVS service that gave the indicated return code is DYNALLOC. To determine the meaning of the return code, refer to *z/OS MVS Programming: Authorized Assembler Services Guide*. Look up the section on dynamic allocation return and reason codes. Dynamic allocation is also known as SVC 99, and may be documented that way. If the problem persists, gather appropriate diagnostic information and contact the IBM support center.

IRRR003I RACF command output transmitted because user data set *data-set-name* format is not correct.

Explanation: Output was returned from one of the following to the issuer via TSO TRANSMIT because the user's output data set does not have the required format.

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

Output data sets must have DSORG=PS, LRECL=80. This message is sent to the user's TSO terminal.

System Action: None.

User Response: If you wish directed command output to be written to a data set, replace your erroneous xxxxxxx.RRSFLIST data set with one that has the required DSORG and LRECL.

IRRR004I RACF command output transmitted because user data set *data-set-name* could not be opened. Abend code is *abend-code*.

Explanation: Output was returned from one of the following to the issuer via TSO TRANSMIT:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

Allocation of the user's output data set failed because the output data set could not be opened for write access.

System Action: None.

User Response: Refer to to determine the specific *z/OS MVS System Codes* cause of the open failure. If you have authorization to the data set, report the

complete text of this message to the system programmer. If you do not have authorization to the data set, contact the RACF security administrator to address the problem of authorization. You will continue to receive returned output via TSO TRANSMIT as long as you cannot open the data set.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

IRRR005I The initial portion of the command output is unavailable.

Explanation: The first portion of the returned output from a directed RACF command was lost. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: Report the complete text of this message to the system programmer or RACF security administrator.

System Programmer Response: One or more records containing the returned output from the command could not be located within the appropriate INMSG workspace file. Gather appropriate diagnostic information and contact the IBM support center.

IRRR006I Command output was truncated at this point.

Explanation: A portion of the returned output from a directed RACF command was lost. This message marks the end of output that was retained. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: Report the complete text of this message to your system programmer or RACF security administrator.

System Programmer Response: One or more records containing the returned output from the command could not be located within the appropriate INMSG workspace file. Gather appropriate diagnostic information and contact the IBM support center.

IRRR007I Command output was resumed at this point.

Explanation: A portion of the returned output from a directed RACF command was lost. This message marks the beginning of output that was retained. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: None.

IRRR008I Command succeeded. There are no messages.

Explanation: The directed RACF command processed successfully at the execution node and generated no output. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: None.

IRRR009I Command ended with return code *return-code*. There are no messages.

Explanation: There was no output from a directed RACF command that failed at the execution node. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: If you suspect that the command failed due to user error, consider reissuing the RACF command. Otherwise, report the complete text of this message to your system programmer or RACF security administrator.

IRRR010I Command was not executed. Processing code *code* was returned by the executing node.

Explanation: A directed RACF command could not be processed due to an error at the execution node. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: If this message indicates a code other than 507, report the complete text of this message to your system programmer or RACF security administrator. If this message indicates a code of 507, retry the command.

Code Function

500	Internal error while trying to execute the command.
507	Task being restarted concurrently.
508	Error while parsing the command.
509	Command not a supported RACF command.
510	Command not supported with the sysplex ROUTE command.
511	Failure in the TSO IKJSCAN service.

Destination: Port the processing code from this message to the IBM service center.

IRRR011I *command* was successful at node *node-name*. Output {written to *data-set-name* | was sent via TSO TRANSMIT | was lost | was not requested}

Explanation: The output from a directed or automatically directed RACF command was received from the execution node. The output was returned to the user in the described manner or could not be returned to the user due to error. If the output was "not requested", the command was automatically directed, the SET AUTODIRECT OUTPUT setting for this user was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was "lost", an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is sent to the user's TSO terminal.

System Action: None.

User Response: Examine your RRSFLIST data set or invoke TSO RECEIVE to view the returned output from the directed command. If the command output could not be returned, a TSO TRANSMIT attempt failed and you should contact your system programmer to report the failure.

IRRR012I *command* was unsuccessful at node *node-name*. Output {written to *data-set-name* | was sent via TSO TRANSMIT | was lost | was not requested}

Explanation: The output from a directed or automatically directed RACF command was received from the execution node. The output was returned to the user in the described manner or could not be returned to the user due to error. If the output was "not requested", the command was automatically directed, the SET AUTODIRECT OUTPUT setting for this user was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was "lost", an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is sent to the user's TSO terminal.

System Action: None.

User Response: Examine your RRSFLIST data set or invoke TSO RECEIVE to view the returned output from the directed command. If the command output could not be returned, a TSO TRANSMIT attempt failed and you

IRRR013I • IRRR017I

should contact your system programmer to report the failure.

IRRR013I **User RRSFLIST data set full. Command output will be sent via TRANSMIT.**

Explanation: The output from a directed RACF command could not be fully written to the user's RRSFLIST data set. The full set of command output is sent to the user as a message via the TSO TRANSMIT command. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: Invoke the TSO RECEIVE command to view the returned output from the directed RACF command. Take the appropriate actions against your RRSFLIST data set, such as allocating a larger data set or deleting lines from the existing data set.

IRRR014I **Command output truncated at execution node maximum of *number* lines.**

Explanation: The first *number* lines of output generated by the directed RACF command were returned by the execution node. Other lines of generated output were not saved during command processing and are not available. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: None.

User Response: None.

IRRR015I *subsystem-name* **SUBSYSTEM COULD NOT TRANSMIT RETURNED OUTPUT BECAUSE {JESNODE NAME IS NOT KNOWN | JOBID HAS NOT BEEN OBTAINED | SVC SCREENING IS NOT IN EFFECT}. RETURNED OUTPUT IS BEING HELD.**

Explanation: RACF normally tries to return directed command output to a user's RRSFLIST data set. If the data set is full or inaccessible, RACF attempts to TRANSMIT the output directly to the user. In this case, RACF needed to TRANSMIT the output to the user, but was not successful for the reason listed in the message. RACF holds this returned output in the appropriate INMSG workspace file indefinitely until it is able to return it via the user's RRSFLIST data set or via TSO TRANSMIT. This message might be seen during RACF subsystem initialization if RACF needs to return output via TSO TRANSMIT and the JESNODE name has not been obtained yet.

System Action: None.

Operator Response: Report the complete text of this

message to the system programmer.

System Programmer Response: If the JOBID has not been obtained and the *subsystem-name* subsystem address space was halted and restarted, ensure that "SUB=MSTR" was specified on the start command so that the necessary JOBID may be obtained by the subsystem.

If the JESNODE name is not known, the SET LIST command may be used to determine if the JESNODE name is known to the subsystem. If it is not known, its value may be supplied via the SET command.

In all other cases, report the issuance of this message to the IBM support center.

Destination: Descriptor code is 6. Routing code is 2.

IRRR016I **Command was not sent. Processing code is *code*.**

Explanation: An error occurred during the propagation of a directed or automatically directed command. The command could not be sent to the intended node. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

Code	Explanation
------	-------------

502	Error obtaining storage
503	Error writing to a workspace data set
504	User ID association does not exist, is not approved, or cannot be retrieved
505	Unknown target node
506	Command too long. The maximum length of a directed command is 5000 bytes.

System Action: The command is not sent to the target node.

User Response: Contact your system programmer.

System Programmer Response: The processing code in the error message indicates what type of error occurred. Check the list of codes in the explanation of this message.

IRRR017I *command* **could not be sent to node *node-name*. Output {written to *data-set-name* | was sent via TSO TRANSMIT | was lost | was not requested}**

Explanation: This message is sent to a user through the TSO SEND command. It is notification of the results of a directed or automatically directed command. The command was intended to be sent to a target node, but an error occurred before the command could be sent. For example, the problem may have occurred while obtaining storage or performing I/O to a workspace data set. If the output was "not requested", the command

was automatically directed, the SET AUTODIRECT OUTPUT setting for this user was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was “lost”, an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is displayed via TSO SEND to the user’s terminal.

User Response: If the command output was returned, check its contents for additional error messages, such as error message IRRR016I. Additional error messages may have been sent to the operator console or records written to SYS1.LOGREC.

IRRR018I *command not processed at node node-name. Output {written to data-set-name | was sent via TSO TRANSMIT | was lost | was not requested}*

Explanation: This message is sent to a user through the TSO SEND command. It is notification of the results of a directed or automatically directed command. The command was sent to a target node, but an error occurred before or during the processing of the command on that node. For example, the target user ID may not exist or is revoked. If the output was “not requested”, the command was automatically directed, the SET AUTODIRECT OUTPUT setting for this user was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was “lost”, an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is displayed via TSO SEND to the user’s terminal.

User Response: If the command output was returned, check its contents for additional error messages, such as error message IRRR010I, IRRR011I, IRRR012I, or IRRR010I. Additional error messages may have been sent to the operator console.

IRRR019I **UNABLE TO ESTABLISH RACF ENVIRONMENT TO PROCESS OUTPUT RECEIVED FROM NODE** *node-name.*

Explanation: The RACF subsystem address space attempted to send command output or results from one of the following on the indicated node to a user on the local node.

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

When establishing the RACF environment for the user, the RACROUTE REQUEST=VERIFY failed, possibly because the user does not exist. This message is accompanied by message IRRR011I, which names the user ID and contains the RACROUTE REQUEST=VERIFY return codes.

System Action: The command output or results are not returned to the intended user.

User Response: Determine why the RACROUTE REQUEST=VERIFY failed, based on the return and reason codes in accompanying message IRRR011I.

If the user ID does not exist (RACROUTE return code is 4 and RACF return code is 4 in message IRRR011I), an incorrect user ID was specified on the SET command on the indicated node. Issue the SET LIST command on the indicated node to display the current OUTPUT and NOTIFY settings for automatic command direction. Note where the incorrect user ID appears and issue the SET command with the appropriate OUTPUT and NOTIFY keywords to correct the error.

If there is some other problem with the user ID (the return codes are different than stated above), report the exact text of this message and accompanying message IRRR011I to your RACF security administrator.

RACF Security Administrator Response: The return and reason codes from RACROUTE REQUEST=VERIFY are documented in *z/OS Security Server RACROUTE Macro Reference*. Based on what the codes indicate (for example, the user ID is revoked), correct the error appropriately (for example, resume the user ID).

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRR020I **Password synchronization unsuccessful at node** *node-name.*
{Output was sent via TSO TRANSMIT. | Output written to *data-set-name.***}**

Explanation: RACF has encountered an error during the processing of a password synchronization request. Output from the password synchronization request has been sent via the TSO TRANSMIT command or written to your RRSFLIST data set. This message is displayed via TSO SEND to the user’s terminal.

System Action: The system continues processing.

User Response: Examine the output from the password synchronization request to determine the nature of the error.

IRRR021I **Password synchronization successful at node** *node-name.* **{Output written to** *data-set-name.* **| Output was sent via TSO TRANSMIT.}**

Explanation: RACF has successfully processed a password synchronization request at the node specified

IRRR080I • IRRR104I

in the message. Output from the password synchronization request has been written to your RRSFLIST data set. This message is displayed via TSO SEND to the user's terminal. This is an informational message.

System Action: The system continues processing.

IRRR080I *subsystem-name* **SUBSYSTEM OUTPUT HANDLING TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS**
returncode-reasoncode.

Explanation: In attempting to return the output from a directed RACF request, a task within the *subsystem-name* subsystem ended abnormally, with the given return and reason codes.

Operator Response: Report the occurrence of the message to the system programmer.

System Programmer Response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6. Routing code is 2.

IRRR101I **Application update request completed successfully for class** *class-name*,
profile name *profile-name.*

Explanation: Profile *profile-name* in class *class-name* has been updated successfully.

System Action: The RACF database has been changed on both the source node and on the target node.

User Response: The RACF database has been changed on both the source node and on the target node.

IRRR102I *request-type* **request unsuccessful, return code** *return-code*, **reason code**
reason-code, **for class** *class-name*,
profile name *profile-name.*

Explanation: Profile *profile-name* in class *class-name* has not been updated, or was not completely updated. The *request-type* is ICHEINTY, RACDEF or RACXTRT, depending on the request that was propagated. The failing request's return code is *return-code* and the reason code is *reason-code*. The return code and reason code are hexadecimal values.

System Action: The RACF database is changed on the source node, but is not changed, or is not completely changed, on the target node.

User Response: Check the RRSFLIST output for additional information, such as the node where the failure occurred, the type of request, and, for ICHEINTY requests, additional ICH51nnnI messages. The failing request's parameter list is also dumped with message

IRRR105I. For RACDEF and RACXTRT requests, the parameter list being dumped is the RACROUTE parameter list generated by RRSF to transport the request to the target node.

IRRR103I **RACROUTE request unsuccessful, RACROUTE return code**
racroute-return-code, **RACF return code**
racf-return-code, **RACF reason code**
racf-reason-code, **for class** *class-name*,
profile name *profile-name.*

Explanation: Profile *profile-name* in class *class-name* was not updated, or has not been completely updated. The failing RACROUTE return code is *racroute-return-code*, the RACF return code is *racf-return-code*, and the RACF reason code is *racf-reason-code*. The return codes and reason code are hexadecimal values.

System Action: The RACF database is changed on the source node, but it is not changed, or is not completely changed, on the target node.

User Response: Check the RRSFLIST output for additional information, such as the node where the failure occurred, and the type of RACROUTE request. It is also possible that the databases are not synchronized. You can determine this by comparing a list of profiles on each system. The failing RACROUTE parameter list is also dumped with message IRRR105I.

IRRR104I *abend-code[-yyy]* **abend during request-type processing for class**
class-name, **profile name** *profile-name.*

Explanation: An abend occurred while processing an application update for profile *profile-name* in class *class-name*. The *request-type* is ICHEINTY, RACROUTE, RACDEF or RACXTRT, depending on the request that was propagated. The failing request abended with a system or user abend as indicated by the *abend-code*, for example SOC4. If a reason code was specified with the abend code, it is displayed as *yyy*.

System Action: The RACF database was changed on the source node, but it might or might not have been changed on the target node.

User Response: Check the RRSFLIST output for additional information, such as the node where the failure occurred. The failing request's parameter list is also dumped with message IRRR105I. For RACDEF and RACXTRT requests, the parameter list being dumped is the RACROUTE parameter list generated by RRSF to transport the request to the target node. A dump might have been produced on the node where the failure occurred. Notify the system programmer for that node.

System Programmer Response: For an explanation of the abend code, see *z/OS MVS System Codes*.

IRRR105I Failing parameter list follows:

Explanation: An error occurred while performing an application update. This message is preceded by IRRR102I, IRRR103I, or IRRR104I, which provide additional information about the error. This message starts a display of a RACROUTE or ICHEINTY macro parameter list. If the error occurs for a RACXTRT or RACDEF, a RACROUTE parameter list is displayed.

System Action: See the system action for the message that precedes this one.

User Response: Examine the request type, return codes, and parameter list provided in the RRSFLIST output. For mappings of the parameter lists to help you determine the cause of the error, see *z/OS Security Server RACF Diagnosis Guide*.

- If the output was "lost," an error occurred while attempting to return the output. For example, a workspace data set was damaged or a TRANSMIT was attempted to the JES *node name*.
- If the output was "not requested," the OUTPUT setting of the SET command did not specify that output should be returned.

User Response: Examine the RRSFLIST data set, *data-set-name*, or invoke TSO RECEIVE to view the returned output. If the output was lost, contact your system programmer and report the failure. If output is available, examine the output for additional diagnostic information, such as the node affected and messages such as IRRR102I or IRRR103I. If a TRANSMIT was attempted to the JES *node name*, use the SET JESNODE command.

**IRRR111I Application update has completed successfully at node *node-name*.
Output {written to *data-set-name* | was sent via TSO TRANSMIT | was lost | was not requested}**

Explanation: The output from an automatically directed application update was received from the execution node. The output was returned in the described manner or could not be returned because of an error.

- The update to the RACF database on the target system was made successfully.
- If the output was "lost," an error occurred while attempting to return the output. For example, a workspace data set was damaged or a TRANSMIT was attempted to the JES *node name*.
- If the output was "not requested," the OUTPUT setting of the SET command did not specify that output should be returned.

User Response: Examine the RRSFLIST data set, *data-set-name*, or invoke TSO RECEIVE to view the returned output. If the output was lost, contact your system programmer and report the failure. If a TRANSMIT was attempted to the JES *node name*, use the SET JESNODE command.

IRRR116I Application update request was not sent for class *class-name*, profile name *profile-name*. Processing code is *code*.

Explanation: An error occurred during the propagation of an automatically directed application update. The update for profile *profile-name* in class *class-name* could not be sent to the intended node. This message appears in the RRSFLIST output based on the OUTPUT setting of the SET command, or is transmitted if the RRSFLIST data set is full.

System Action: The RACF database is changed on the source node, but is not changed on the target node.

User Response: Contact your system programmer.

System Programmer Response: The processing code in the error message indicates what type of error occurred. They are as follows:

Code	Explanation
502	Error obtaining storage
503	Error writing to a workspace data set
506	Update parameter list is too long

**IRRR112I Application update has completed unsuccessfully at node *node-name*.
Output {written to *data-set-name* | was sent via TSO TRANSMIT | was lost | was not requested}.**

Explanation: The output from an automatically directed application update was received from the execution node. The output was returned in the described manner or could not be returned because of an error.

- The update to the RACF database on the target system was not made successfully. It failed either partially or completely.

IRRR117I Application update could not be sent to node *node-name*. Output {written to *data-set-name* | was sent via TSO TRANSMIT | was lost | was not requested}.

Explanation: This message is sent to a user through the TSO SEND command. It is notification of the results of an automatically directed application update. The update was intended to be sent to a target node, but an error occurred before the update could be sent. For example, the problem might have occurred while obtaining storage or performing I/O to a workspace data set.

- If the output was "lost," an error occurred while attempting to return the output. For example, a

IRRR118I • IRRS001I

workspace data set was damaged or a TRANSMIT was attempted to the JES node name.

- If the output was "not requested," the OUTPUT setting of the SET command did not specify that output should be returned.

User Response: If output was returned, check its contents for additional error messages, such as error message IRRR116I. There might also be additional error messages sent to the operator console or records written to the LOGREC data set. If a TRANSMIT was attempted to the JES node name, use the SET JESNODE command.

IRRR118I **Application update could not be executed at node *node-name*. Output {written to *data-set-name* | was sent via TSO TRANSMIT | was lost | was not requested}.**

Explanation: This message is sent to a user through the TSO SEND command. It is a notification of the results of an automatically directed application update. The update was sent to a target node, but an error occurred before the processing of the update on that node. For example, the target user ID might not exist or is revoked.

- If the output was "lost," an error occurred while attempting to return the output. For example, a workspace data set was damaged or a TRANSMIT was attempted to the JES *node name*.
- If the output was "not requested," the OUTPUT setting of the SET command did not specify that output should be returned.

User Response: If output was returned, check its contents for additional error messages, such as error message IRRR110I, IRRR011I, or IRRR012I. There might also be additional error messages sent to the operator console or the syslog. If a TRANSMIT was attempted to the JES *node name*, use the SET JESNODE command.

IRRR119I **APPLICATION UPDATE *type* CANNOT BE SENT TO PARTNER NODE *node-name* [SYSNAME *system-name*]. THIS PARTNER NODE HAS RACF LEVEL *level* WHICH DOES NOT SUPPORT AUTOMATIC DIRECTION OF APPLICATION UPDATES.**

Explanation: An attempt was made to propagate an application update, or to return output from an

application update to a downlevel remote node.

If *type* is REQUEST, the application update could not be sent to the remote partner node indicated by the RRSFDATA profiles.

If *type* is OUTPUT, the output produced by an application update could not be sent to the remote partner node specified by the SET command. On the last handshake with this node, the level of RACF was not high enough to accept application update requests or output. The level must at least correspond to FMID HRF2230, which is available with the OS/390 Release 3 Security Server. If SYSNAME information is present for the node name in this message, the node that precedes the SYSNAME is a multisystem node.

System Action: If *type* is REQUEST, the RACF database is changed on the source node, but the request is not sent to the target node.

If *type* is OUTPUT, the output produced by an application update attempted on this node is not sent to the node specified by the SET command. The application update may or may not have been successfully made on this node. Additional requests and output directed to this remote partner node are discarded without any additional error messages.

If handshaking occurs again between these nodes, another error message is issued if the remote node is still at a lower level and has requests or output being directed to it.

System Programmer Response: If *type* is REQUEST, you should change the RRSFDATA profiles to prevent automatic direction of application updates to this remote node until it has been updated to a level of RACF that supports these requests. For additional information on RRSFDATA profiles, see *z/OS Security Server RACF Security Administrator's Guide*.

If *type* is OUTPUT, use the SET command to prevent additional output from being sent to this remote node. For additional information on the SET command, see *z/OS Security Server RACF Command Language Reference*.

After the remote system is updated, you need to reestablish the connection with it by issuing a RESTART or TARGET command to pick up the new level.

Destination: Descriptor code is 6. Routing codes are 2 and 9.

RACLINK command messages

IRRS001I **RACF subsystem return code is *return-code*, reason code is *reason-code*.**

Explanation: A problem occurred with the RACF subsystem while processing a RACLINK request. This

message is preceded by a message indicating what problem occurred. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops.

User Response: Refer to the documentation for the error message that was issued before this message.

IRRS002I RACF subsystem is not active, your request cannot be processed.

Explanation: The RACF subsystem has to be active for a RACLINK command to be processed. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops.

User Response: Contact the system operator to start the RACF subsystem.

Operator Response: Start the RACF subsystem by issuing `START subsystem-name,SUB=MSTR` from the operator's console, where *subsystem-name* is the RACF subsystem that you want to become active.

IRRS003I Unable to communicate with the RACF subsystem. IEFSSREQ return code is return code.

Explanation: The RACLINK command attempted to send a request to the RACF subsystem, but the request failed. No profiles have been updated. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: RACLINK command processing ends.

User Response: Report this message to your system programmer.

System Programmer Response: The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

Code	Explanation
4	The subsystem does not support this function.
8	The subsystem exists, but is not active.
12	The subsystem is not defined in the IEFSSNxx parmlib member.
16	The function has not completed. This is a disastrous error.
20	The SSOB or SSIB have invalid lengths or formats.
24	The SSI has not been initialized.

A return code of 4, 16, 20, or 24 indicates of a RACF code problem, report this message to IBM support.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See *z/OS Security Server RACF System Programmer's Guide* for information on configuring the RACF subsystem.

IRRS004I You are not authorized to use the {DEFINE | PWSYNC} keyword for node node-name. The association for userid userid with node.userid was not defined.

Explanation: The RACLINK command issuer is not authorized to use the indicated keyword. The command issuer either has not been permitted to the RACLINK resource's DEFINE or PWSYNC profile, or the RRSFDATA class is not currently active. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops. No user ID association is defined.

User Response: Contact the RACF security administrator to permit you to the RACLINK.DEFINE.*node-name* profile or the RACLINK.PWSYNC.*node-name* profile in the RRSFDATA class and to ensure that the RRSFDATA class is active.

RACF Security Administrator Response: Permit the command issuer to the RACLINK.DEFINE.*node-name* profile or the RACLINK.PWSYNC.*node-name* profile in the RRSFDATA class and issue a SETROPTS command to activate the RRSFDATA class.

IRRS005I RACLINK to associate userid userid with node.userid failed. Associations to the same userid on the same node are not permitted.

Explanation: A RACLINK DEFINE command was issued to define an association with the same user ID on the same node. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops. No user ID association is defined.

IRRS006I The local node is not defined. RACLINK command cannot be processed.

Explanation: RACF is unable to locate the local node. The local node is required for one of the following reasons:

1. To validate the use of the DEFINE keyword and the PWSYNC operand
2. As the command default, because the RACLINK command did not specify a target node.

This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops. No user ID association is defined.

User Response: Contact your RACF security administrator to have the local node defined to the RACF remote sharing facility.

RACF Security Administrator Response: Call the

IRRS007I • IRRT004I

system operator to issue the TARGET command to identify the local node.

IRRS007I The RACLINK command must be authorized.

Explanation: An attempt was made to issue the RACLINK command, but RACLINK is not recognized as an authorized command. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: The RACLINK command being processed is unsuccessful; processing ends.

User Response: Contact the system programmer.

System Programmer Response: The most likely cause of this problem is that RACLINK is not present in the list of authorized commands in the IKJTSOxx parmlib member currently in effect. Another possibility is that RACLINK is not in an APF-authorized library.

IRRS008I YOU ARE NOT ALLOWED TO ISSUE THE RACLINK COMMAND AS AN OPERATOR COMMAND.

Explanation: You issued a RACLINK command as an operator command, but did not have authority for one of the following reasons:

- There is no RACF-defined user ID associated with the operator.
- A profile in the OPERCMDS class is preventing the RACLINK command from being issued by the user ID.

System Action: Processing for this RACLINK command stops.

User Response: If the RACLINK command was issued from an operator console, make sure the console is logged on. If the RACLINK command was issued through some other means, make sure the command is issued from a RACF-defined user ID.

If you received an ICH408I message before this message, an OPERCMDS profile is preventing access. Contact your RACF security administrator to get access to the OPERCMDS profile.

RACF Security Administrator Response: If appropriate, permit the user ID to the OPERCMDS profile that is protecting the RACLINK command.

Destination: Descriptor code is 6. Routing code is 2.

IRRS080I RACF RACLINK command encountered an error. Abend code is *abend-code* - *reason-code*.

Explanation: The RACLINK command abended during RACLINK processing. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops.

User Response: Contact your system programmer.

System Programmer Response: Check the RACLINK abend code supplied with the message and analyze the system dump.

IRRS081I RACF RACLINK command terminated in abend processing.

Explanation: The RACLINK command abended and, during abend processing, the abend handler abended. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops.

User Response: Contact your system programmer.

System Programmer Response: Check the system dump to diagnose the problem.

RACLINK command or RRSF output handling task messages

IRRT003I The (*node.userid1*) association could not be located in the *userid2* user profile.

Explanation: A command was issued to retrieve user ID association information for *node.userid1*, but no user ID association for *node.userid1* was located in the profile for *userid2*. This message is sent to the command issuer or the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: Verify that the correct node and user ID were entered on the command. If they are incorrect, issue the command again with the correct node and

user ID. If the node and user ID are correct and you receive this message, the user ID association must be defined before the command is successful.

IRRT004I The requested association could not be {located | defined | deleted} because user *userid* is not RACF defined.

Explanation: A command was issued to retrieve user ID association information for *userid*, but the *userid* profile does not exist in the RACF database. This message is sent to the command issuer or the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is

unsuccessful; processing ends.

User Response: Verify that the correct *userid* was specified on the command. If incorrect, issue the command again with the correct user ID. If the *userid* is correct, contact the security administrator to add the user ID to the database, if needed.

IRRT005I RACF ICHEINTY return code
return-code received while attempting
to {retrieve | define | delete | approve}
association (node.userid) for user
userid.

Explanation: A command was issued to update or retrieve user ID association information for *node.userid* and an ICHEINTY failure occurred. This message is sent to the command issuer or the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: Verify that the correct command was entered. If incorrect, issue the command again with the correct user ID association information. If the correct command was entered, contact the system programmer.

System Programmer Response: See *z/OS Security Server RACF Macros and Interfaces* to analyze the ICHEINTY return code.

IRRT006I Association key length *length* is not
valid. Information cannot be retrieved
for user *userid*.

Explanation: In the command to retrieve user ID association information for user *userid*, the specified target node or target user ID exceeded the maximum length of 8 characters. This message is sent to the command issuer or the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: Reissue the command with the correct target node and user ID.

IRRT007I No associations could be located in
the *userid* user ID profile.

Explanation: There are no target user ID entries in the indicated user ID profile. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: RACLINK command processing ends and no retrieval is performed.

User Response: Create the required associations with the RACLINK DEFINE command.

IRRT008I Unable to find association(s) which
matched (node.userid1) for user ID
userid2.

Explanation: No target user ID entries match the selection criteria in *userid2*'s profile. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: RACLINK command processing ends and no retrieval is performed.

User Response: Create the required associations with the RACLINK DEFINE command.

IRRT009I RACLINK could not be completed
because target node *node-name* is
undefined.

Explanation: RACF is unable to locate the node name specified. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: The RACLINK command stops processing.

User Response: Issue a RACLINK LIST command to determine if the association is defined or updated. Also, ensure that you spelled the node name correctly. If the node name and its associations are correct, contact your system programmer to have the remote node defined to RACF.

System Programmer Response: Issue the TARGET command to identify the remote node.

IRRT010I The definition for association
(node-name.userid) in user *userid* profile
already exists.

Explanation: The user ID association that you are trying to define already exists in the RACF database. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: Processing for this RACLINK command stops.

User Response: Verify that the correct RACLINK command was entered.

IRRT011I {*command-name* | Password
synchronization} was not performed by
userid at node *node-name*.

Explanation: RACF processing has determined that the indicated function could not be performed at target node *node-name* for target user *userid*. This message is accompanied by messages IRRT003I, IRRT004I, IRRT005I, IRRT006I, IRRT012I, or IRRT013I, which provide a more detailed analysis of the error. Refer to these messages for further details. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

IRRT012I • IRRT016I

System Action: The command being processed is unsuccessful; processing ends.

User Response: Verify that the correct command was entered. If it is correct, refer to the accompanying messages for more information.

IRRT012I Association (*node.userid*) has not been approved.

Explanation: RACF processing has determined that a directed command could not be performed because the user ID association between the command issuer and target user *userid* on target node *node* has not been approved. This error occurs only when user ID association approval processing could not complete as the result of a communication failure between the participating systems. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: Reestablish a user ID association between the user IDs by deleting and then redefining the association. If the user ID association cannot be reestablished, contact the system programmer. The source of the communication failure needs to be determined. If the association was reestablished successfully, retry the command.

System Programmer Response: Communication from the target node to the source node for a directed command has been disrupted. Determine the status of the communication links from the target to the source node by issuing the TARGET LIST command on the target node. If either node is not in the OPERATIVE ACTIVE state, try to put the affected node into the operative state by issuing the TARGET command. The specific command operands depends on the state of the node. See *z/OS Security Server RACF Command Language Reference* for details of the TARGET command.

If communication cannot be reestablished, there is most likely a problem with the physical linkage between the systems.

IRRT013I The ONLYAT keyword was specified but user ID *userid* at node *node-name* does not have the SPECIAL attribute.

Explanation: RACF processing has determined that a directed command could not be performed because the ONLYAT keyword was specified and target user *userid* at node *node-name* does not have the SPECIAL attribute. If the ONLYAT keyword is specified, the command can be directed only to a user who has the SPECIAL attribute. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is

unsuccessful; processing ends.

User Response: Only communication between two user IDs with the SPECIAL attribute is permitted with the ONLYAT keyword. Contact the security administrator on the indicated node *node-name* to determine whether *userid* should be given the SPECIAL attribute.

IRRT014I RACLINK command was unable to obtain storage for the association entry.

Explanation: A failure occurred while attempting to obtain storage necessary to update an association entry in the local user's profile. This message is sent to the RACLINK issuer.

System Action: RACLINK command processing ends. Neither the local user profile nor the remote user profile has been updated.

User Response: Notify the system programmer.

System Programmer Response: Note the message ID and any other diagnostic information generated, and contact your IBM support center.

Problem Determination: The storage request was for subpool 1.

IRRT015I {Peer | Managed} association with *userid* at node *node-name* has been approved.

Explanation: The indicated association with the target user ID was approved. Remote sharing requests to the target user ID can now be processed. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: The RACLINK command completes processing.

User Response: None.

IRRT016I The ONLYAT keyword was specified but user ID *userid* at node *node-name* is not RACF defined.

Explanation: RACF ONLYAT keyword processing has determined that a command cannot be directed to *userid* at node *node-name* because *userid* is not defined to RACF. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: Verify that the correct user ID was specified on the command. If incorrect, issue the command again with the correct user ID. If *userid* is correct, then contact the security administrator to add the user ID to the database.

**IRRT017I *userid* ATTEMPTED TO ACCESS
ASSOCIATION INFORMATION FOR
for-user. ACCESS IS DENIED.**

Explanation: The user *userid* entered a RACLINK command, specifying *for-user* for the ID keyword. User *userid* is not authorized to access the *for-user* profile.

System Action: RACLINK command processing ends. No profiles are updated.

Operator Response: Notify the security administrator.

RACF Security Administrator Response: If *userid* should have the authority to access the *for-user* profile, *userid* must have one of the following authorities:

- System SPECIAL
- SPECIAL in the group that the *for-user* belongs to
- OWNER of the *for-user* profile

Destination: Descriptor code is 4. Routing code is 9.

**IRRT018I Association *node.userid* cannot be
approved. It is not pending approval by
source-userid on node
source-node-name.**

Explanation: The user *source-userid* on node *source-node-name* entered a RACLINK APPROVE command, specifying *node.userid* as the target of the command. This association is not waiting approval by user ID *source-userid* on node *source-node-name*. The association is either already established or is waiting approval from *node.userid*. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: RACLINK command processing ends. No profiles are updated.

User Response: Use the RACLINK LIST command to list the association. From the output, determine if the association is already approved or waiting approval from the target. If it is already approved, no action is required. If it is awaiting approval from the target, contact the target user and request approval for the association.

**IRRT021I Association (*node-name.userid*) deleted
from *userid* user ID profile.**

Explanation: The RACLINK association for the specified node and user ID has been deleted from the RACF database. This message is sent to the TSO terminal of the RACLINK issuer.

System Action: The RACLINK association entry is deleted from the RACF database.

**IRRT024I Your *userid* *userid* does not have
sufficient authority to access the
association information of *userid*.**

Explanation: The RACLINK command failed because the user did not have system SPECIAL, group SPECIAL for the group that owns the user ID specified on the ID keyword, and is not the owner of the user ID specified on the ID keyword. This message is sent to the RACLINK issuer.

System Action: RACLINK command processing ends.

User Response: If you need authority to issue the RACLINK command with the ID keyword or to access the association information for user *userid*, contact your RACF security administrator.

**IRRT026I RACLINK command failure.
Unexpected request *request* was
received. Reason code is *reason-code*.**

Explanation: An internal error occurred while processing a RACLINK request. This message is sent to the RACLINK issuer.

System Action: RACLINK command stops processing.

User Response: Contact the IBM support center to report the problem.

Code	Explanation
1	Define processing received an unknown request.
2	General RACLINK processing received an unknown request.

**IRRT030I RACLINK PROCESSING ERROR.
{INPUT IS NOT CORRECT | REQUEST
TYPE IS NOT CORRECT }**

Explanation: The input to the RACLINK task handler is not correct. Typical causes are:

- Input specified on the RACLINK command was incorrect.
- The request type received was not RACLINK-related.

There may be an internal problem.

System Action: Processing for this RACLINK command stops.

User Response: Contact your system programmer.

System Programmer Response: Contact the IBM service center to report this problem.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRT031I **RACLINK command awaiting approval from *userid* at this node. Association requested by *node-name.userid*.**

Explanation: The RACLINK association is pending approval from the specified user ID. This message is sent to the RACLINK issuer.

System Action: The RACLINK command is on hold until approval.

User Response: Wait until the RACLINK association is approved or contact the owner of the user ID to issue the approval.

Problem Determination: For information on the pending association waiting for your approval, use the RACLINK LIST function.

IRRT032I **RACLINK command to associate user ID *userid* with *node-name.userid* is pending approval.**

Explanation: The RACLINK association is pending approval from the specified user ID. The association could be pending for one of the following reasons:

- The association is waiting approval from the target.
- The conversation between the local and target nodes is not active.
- The RACLINK command is pending for some other reason. A message will follow.

This message is sent to the RACLINK issuer.

System Action: The RACLINK command continues processing. If the target node is not active, the RACLINK request is held in the OUTMSG file until the node is made OPERATIVE. After the node becomes OPERATIVE, the RACLINK command continues processing.

User Response: Other messages usually follow this one indicating the status of the RACLINK request. If no other messages follow, contact the owner of the target user ID to determine if the RACLINK request reached the target user ID. If the RACLINK request reached the target user ID, the target user ID can approve the association using the RACLINK APPROVE command. If the RACLINK request did not reach the target user ID, then the request is most likely queued until the target node is made active. To determine the status of the target node, contact the system programmer.

System Programmer Response: Query the status of the communication link between the two nodes by issuing the TARGET LIST command. The node must be made OPERATIVE in order for the RACLINK request to be processed.

IRRT033I **The local node is not defined. RACLINK command cannot be processed.**

Explanation: RACF is unable to locate the local node. This message is sent to the RACLINK issuer.

System Action: The RACLINK command stops processing. No user ID association is defined.

User Response: Verify that this is the correct node to be sending commands to. If it is, contact your system programmer to have the local node defined to RACF.

System Programmer Response: Issue the TARGET command to identify the local node.

IRRT034I **All associations of RACLINK command issuer not sent to target node *node-name*. Number associations were sent.**

Explanation: There is a limit to the number of user IDs that may be sent to the target node at one time. That limit is indicated by *number* in the message. This message is sent to the RACLINK issuer.

User Response: To determine what user IDs were sent to the target node, issue the RACLINK LIST command to display the user ID associations of the user ID. The display shows the user ID and node of each association. The first *number* user IDs on the indicated *node-name* were sent to the target node. If the association did not get approved, the target user must issue a RACLINK APPROVE command.

IRRT042I ***subsystem-name* SUBSYSTEM WAS UNABLE TO ISSUE IEFSSREQ REQUEST. RETURN CODE IS: *return-code*.**

Explanation: The RACLINK command attempted to send a request to the MVS IEFSSREQ subsystem and the request failed. No profiles have been updated.

System Action: RACLINK command processing ends.

User Response: Report this message to your system programmer.

System Programmer Response: The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

Code	Function
4	The subsystem does not support this function.
8	The subsystem exists, but is not active.
12	The subsystem is not defined in the IEFSSNxx parmlib member.
16	The function has not completed. This is a disastrous error.

- 20** The SSOB or SSIB have incorrect lengths or formats.
- 24** The SSI has not been initialized.

A return code of 4, 16, 20 or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See *z/OS Security Server RACF Migration* for installation considerations and *z/OS Security Server RACF System Programmer's Guide* for configuration considerations for the RACF subsystem.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRT043I *subsystem-name* **SUBSYSTEM IEFSSREQ REQUEST ENDED WITH A RETURN CODE OF** *return-code*.

Explanation: An attempt to send a request to the MVS IEFSSREQ subsystem interface failed. No profiles have been updated.

System Action: RACLINK command processing ends.

Operator Response: Report this message to your system programmer.

System Programmer Response: The return code indicated in this message is the value of the SSOBRETN field in the subsystem's option block (SSOB). The return code may be one of these values:

Code Explanation

- 8** The subsystem could not execute the command because of an internal parameter error, or the subsystem supports this request, but is not active.
- 16** The caller is not APF-authorized, or storage is not available for an internal data area.

Contact the IBM support center to report this problem.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRT080I *subsystem-name* **SUBSYSTEM RECEIVE REQUEST HANDLING TASK ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code - reason-code*.

Explanation: An abend occurred during the receive of a RACF remote sharing facility request from another address space. This message is written to the SYSLOG.

System Action: The receive request handler attempts to retry the current work request.

Operator Response: Report this message to your system programmer.

System Programmer Response: The message contains the abend code, for example 0C1, and a reason code. See *z/OS MVS System Codes* for an explanation of these codes.

File allocation messages

IRRU080I *subsystem-name* **RACF VSAM FILE OPEN AND CLOSE PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*.

Explanation: The subsystem task that holds all the VSAM OPENs for the subsystem encountered an error. This message is written to the SYSLOG.

System Action: The task attempts to restore an operational state by ignoring the current request and moving to the next request.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see *z/OS Security Server RACF Diagnosis Guide*.

Operator Response: Report this message to your system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

IRRU081I *subsystem-name* **RACF VSAM FILE OPEN AND CLOSE PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS** *abend-code*. **PROGRAM ENDING.**

Explanation: The subsystem task that holds all the VSAM OPENs for the subsystem had an error.

This message appears when an abnormal situation that cannot be recovered from occurs.

System Action: The program releases all system resources it holds, this includes closing all VSAM files, posting all tasks waiting on this program and then ends. The subsystem attempts to restart the file program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see *z/OS Security Server RACF Diagnosis Guide*.

Operator Response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see *z/OS MVS System Codes*.

Destination: Descriptor code is 6. Routing code is 2.

RRSF enveloping messages

IRRV001I RACF command envelope ended in abend processing.

Explanation: An internal error occurred. RACF experienced an abend while handling a prior abend. The initial abend code should be listed in message IRRV080, which was issued before this one. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued, or this message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: Processing is halted at the time of the abend.

User Response: If you were performing an update type command (for example, ALTUSER), you can use the appropriate list command (for example, LISTUSER) to determine if the update occurred prior to the abend. If the problem persists, contact your RACF support personnel and report the abends to the IBM support center. Be sure to indicate the abend code and reason code that were reported in the message.

Problem Determination: Examine the console log and the system abend dump for more information pertaining to the abends.

IRRV002I Node *nodename* is not defined to RACF or is not available.

Explanation: An attempt was made to direct a RACF command to a node that has not been defined or that is not available. *nodename* might appear as an asterisk (*) if you used shorthand notation to direct a command to the local node (for example, AT(.userid)) and had not defined a local node. This message is sent to the user's TSO terminal.

System Action: This message is followed by message IRRV005I, which indicates that the command will not be sent to node *nodename*. If the AT (or ONLYAT) keyword specified other nodes that are defined and available, the command is still processed on those nodes.

User Response: If you made an error while entering the node name, reissue the command with the correct node name. Otherwise, contact your RACF security administrator to determine whether the node is defined and, if so, why it is not available.

Problem Determination: If you are authorized to issue RACF operator commands, you can issue the TARGET LIST command to determine which nodes are defined to your system.

IRRV003I YOU ARE NOT ALLOWED TO ISSUE THE *command* COMMAND AS AN OPERATOR COMMAND.

Explanation: You issued a RACF command as an operator command, but did not have authority for one of the following reasons:

- There is no RACF-defined user ID associated with the operator.
- A profile in the OPERCMDS class is preventing the command from being issued by the user ID.

Note: If the command you entered was a SETROPTS command, you may have READ access, which only allows you to issue SETROPTS LIST. You need to have UPDATE access to issue the SETROPTS command with keywords other than LIST.

System Action: Processing for this command stops.

User Response: If the command was issued from an operator console, make sure the console is logged on. If the command was issued through some other means, make sure the command is issued from a RACF-defined user ID.

If you received an ICH408I message before this message, an OPERCMDS profile is preventing access. Contact your RACF security administrator to get access to the OPERCMDS profile.

RACF Security Administrator Response: If appropriate, permit the user ID to the OPERCMDS profile that is protecting the command in question.

Destination: Descriptor code is 6. Routing code is 2.

IRRV004I Unexpected return code *return-code* received from node name and user ID verification.

Explanation: Because of an internal error, RACF was unable to properly verify the node name and user ID being processed. This message is issued from the IRRENV04 CSECT when an unknown return code is returned from the node name and user ID verification service. This message is sent to the user's TSO terminal.

System Action: This message is followed by message IRRV005I, which indicates that the command will not be sent to the specified node. If the AT (or ONLYAT) keyword specified other nodes to direct the command to, those other nodes are still processed.

User Response: Try directing the command again to the node and user ID. If it fails, contact your RACF support personnel and report the problem to the IBM

support center. Be sure to indicate the return code from this message.

IRRV005I **Command RACF-command will not be sent to node *nodename*.**

Explanation: An error prevented RACF from directing the command to the specified node. This message follows another message that describes in more detail why the command will not be sent. *nodename* might appear as an asterisk (*) if you used shorthand notation to direct a command to the local node (for example, AT(.userid)) and had not defined a local node. This message is sent to the user's TSO terminal.

System Action: The command is not sent to the specified node. If the AT (or ONLYAT) keyword specified that the command be directed to other nodes, those other nodes are still processed.

User Response: See the message that was issued before message IRRV005I. It should describe why the command was not sent.

IRRV006I **Unexpected return code *return-code* received from the parse of command RACF-command.**

Explanation: RACF was not able to properly parse the command due to an internal logic error. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued, or this message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: The command ends processing.

User Response: Contact your RACF support personnel and report the problem to the IBM support center. Be sure to indicate the return code from this message and any other associated messages.

IRRV007I **Node *nodename* is not active.**

Explanation: An attempt was made to direct a RACF command to a node that is not currently active. This message is for your information only to warn you that there may be a delay before the command actually runs at the target node. This message is sent to the user's TSO terminal.

System Action: RACF sends the command request to the RACF subsystem where it will be saved. Message IRRV008I follows this message to indicate that the command will be saved. Once the target node is made operative, the saved commands will be processed. Your commands will be processed in the same order as you issued them.

User Response: None required. However, if you need the RACF command change to take effect immediately, do one of the following:

- Contact the system programmer to activate the node.
- Issue the command directly on the target system. This requires you to log on to the target node and issue the command without the AT (or ONLYAT) keyword.

IRRV008I **Command RACF-command will be queued for later transmission to node *nodename*.**

Explanation: This message is for your information only to warn you that there may be a delay before the command actually runs at the target node. Message IRRV007I, which was issued before this message, should tell you why the command is being queued. This message is sent to the user's TSO terminal.

System Action: RACF sends the command request to the RACF subsystem where it will be saved.

User Response: None required. However, if you need the RACF command change to take effect immediately, do one of the following:

- Have your RACF personnel make the target node operative so the command runs.
- Issue the command directly on the target system. This requires you to log on to the target node and issue the command without the AT (or ONLYAT) keyword.

IRRV009I **Authorization failed for the ONLYAT keyword.**

Explanation: The ONLYAT keyword was specified, but you are not authorized to use it. The following requirements must be met for you to specify the ONLYAT keyword:

- You must have RACF system SPECIAL authority.
- The target user ID must have RACF system SPECIAL authority.
- If the target user ID is different from your user ID, a user ID association between your user ID and the target user ID is required.

This message is sent to the user's TSO terminal.

System Action: Command processing fails to complete.

User Response: Ensure all of the above requirements are met and reissue the command.

IRRV012I **Association exists, but has not been approved.**

Explanation: An attempt was made to direct a RACF command to a remote node. To direct such a command, you must have an approved association between the issuing user ID on the source node and the target user ID on the remote node. In this case, an association does exist between the user IDs, but the association

IRR013I • IRR015I

has not been approved. This message is sent to the user's TSO terminal.

System Action: This message is followed by message IRR005, which indicates that the command will not be sent to the specified node. If the AT (or ONLYAT) keyword specified other nodes to direct the command to, those other nodes are still processed.

User Response: If you made a typo while entering the node name or target user ID, reissue the command and enter the correct node name and target user ID. Otherwise, if the association is valid (that is, both parties agree it should be allowed), you need to have the association approved. If you have the authority, use the RACLINK LIST command to determine who must approve the association. If you need to approve the association, use the RACLINK command to APPROVE the association. If you do not have the authority, contact your administrator or the target user and have them use the RACLINK command to APPROVE the association.

If you need more information on the authorization requirements for using the ONLYAT keyword, see *z/OS Security Server RACF Security Administrator's Guide*.

Problem Determination: Use the RACLINK command to LIST the associations for the user ID. This can be done on each system to see what state each system thinks the relationship is in. Remember to use the ID() keyword to LIST the association if the association is for a user ID other than your own. If you try the RACLINK command with the APPROVE keyword, and the RACLINK LIST command still shows the association as PENDING APPROVAL, you should contact your RACF support personnel and report the problem to the IBM support center.

IRR013I *subsystem-name* **SUBSYSTEM**
RACF-command **COMMAND FROM THE**
{RACF PARAMETER LIBRARY |
OPERATOR CONSOLE | IRRSEQ00
CALLABLE SERVICE} WAS NOT
PROCESSED.

Explanation: An attempt was made to run a command containing the AT or the ONLYAT keyword in the RACF parameter library, from the operator console, or from the IRRSEQ00 callable service. These keywords cannot be used to direct commands that run in the RACF parameter library or are entered from the operator console or the IRRSEQ00 callable service.

System Action: The command is ignored. Message IRR014I is also issued to provide more information.

User Response: If the command is in the RACF parameter library, remove the command from the RACF parameter library. If you wish the command to run automatically, you must remove the AT or ONLYAT keyword and place the command in the RACF parameter library of the system you would like it to execute on.

If the command was entered from the operator console, issue the command from TSO, or issue the command without the AT or ONLYAT keyword from an operator console attached to the system where it is supposed to execute.

If the command was entered from the IRRSEQ00 callable service, issue the command from the callable service without the AT or ONLYAT keyword.

Destination: Descriptor code is 6. Routing code is 2.

IRR014I *subsystem-name* **SUBSYSTEM AT() OR**
ONLYAT() KEYWORDS MAY NOT BE
SPECIFIED WITH COMMANDS FROM
THE {RACF PARAMETER LIBRARY |
OPERATOR CONSOLE | IRRSEQ00
CALLABLE SERVICE}.

Explanation: An attempt was made to run a command containing the AT or the ONLYAT keyword in the RACF parameter library, from the operator console, or from the IRRSEQ00 callable service. These keywords cannot be used to direct commands that run in the RACF parameter library or are entered from the operator console or the IRRSEQ00 callable service.

System Action: The command is ignored. Message IRR013I is also issued to provide more information.

User Response: If the command is in the RACF parameter library, remove the command from the RACF parameter library. If you wish the command to run automatically, you must remove the AT or ONLYAT keyword and place the command in the RACF parameter library of the system you would like it to execute on.

If the command was issued from the operator console, issue the command from TSO, or issue the command without the AT or ONLYAT keyword from an operator console attached to the system where it is supposed to execute.

If the command was issued from the IRRSEQ00 callable service, issue the command from the callable service without the AT or ONLYAT keyword.

Destination: Descriptor code is 6. Routing code is 2.

IRR015I **You are not authorized to direct**
commands to the *nodename* node with
the AT() keyword.

Explanation: You attempted to direct a RACF command to a RACF node via the AT() keyword, but are not authorized to do so. This message is sent to the user's TSO terminal.

System Action: The command is not be sent to the specified node. If the AT keyword specified other nodes to direct the command to, those other nodes are still processed.

User Response: Contact your RACF security

administrator. The users that are allowed to use the AT keyword are determined by the installation.

Problem Determination: The ability to direct commands with the AT keyword is protected via RACF profiles in the RRSFDATA class. Ensure that the RRSFDATA class is active, profiles are up to date (that is, RACLIST REFRESHed if you have the class RACLISTed), and that you have the proper authority granted to the profile covering the "DIRECT.nodename" entity. For more details, see *z/OS Security Server RACF Security Administrator's Guide*.

IRR016I Unable to communicate with the RACF subsystem. IEFSSREQ return code is return-code.

Explanation: An internal error occurred. RACF received an unexpected return code while attempting to communicate with the RACF subsystem. The communication is via the JES subsystem interface service provided via the IEFSSREQ macro. This message is sent to the user's TSO terminal.

System Action: Processing is halted after the unexpected return code is received. Message IRR017I follows and informs the issuer that the command cannot be sent to the target node.

User Response: In most cases the command is not directed to the target nodes. If you were directing the command to multiple nodes, it is possible for you to get stuck in a timing situation where the first target was processed, and the second one was not. In this case, you may use the appropriate list command (for example, LISTUSER) to determine if the update occurred on any specific node. Reissue the command. If the problem persists, notify the system programmer.

System Programmer Response: The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

Code	Explanation
4	The subsystem does not support this function.
8	The subsystem exists, but is not active.
12	The subsystem is not defined in the IEFSSNxx parmllib member.
16	The function has not completed. This is a disastrous error.
20	The SSOB or SSIB have invalid lengths or formats.
24	The SSI has not been initialized.

A return code of 4, 16, 20 or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See *z/OS Security Server RACF Migration* for installation considerations and *z/OS Security Server RACF System Programmer's Guide* for configuration considerations for the RACF subsystem.

IRR017I Command RACF-command will not be sent to the requested node(s).

Explanation: An internal error occurred. RACF received an unexpected return code while attempting to communicate with the RACF subsystem. The communication is via the JES subsystem interface service provided via the IEFSSREQ macro. This message is sent to the user's TSO terminal.

System Action: Processing is halted after the unexpected return code is received. Message IRR016I should precede this message and indicate the IEFSSREQ return code received.

User Response: In most cases, the command is not directed to the target nodes. If you were directing the command to multiple nodes, it is possible for you to get stuck in a timing situation where the first target was processed, and the second one was not. In this case, you may use the appropriate list command (for example, LISTUSER) to determine if the update occurred on any specific node. Reissue the command. If the problem persists, contact your RACF support personnel and report the return code.

Problem Determination: If you are receiving return code 4, it is likely that someone at your installation has shut down the RACF subsystem. Contact your RACF support personnel and report the return code. If you are receiving another return code, look it up in *z/OS MVS Using the Subsystem Interface*. If you have never had the RACF subsystem successfully running, this may help you determine the problem. If you have had it running and this problem just surfaced, report it to the IBM support center. Be sure to indicate the return code that was reported in the message.

IRR018I Commands cannot be directed to the manager of a user ID association.

Explanation: The target user ID of a directed command is the manager of the user ID association between the command issuer and the target user ID. The managed user ID cannot direct a command to the manager of the user ID association. This message is sent to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: If command direction between the two user IDs is desired, redefine the association as peer if you have sufficient authority, or contact the security administrator.

**IRRV019I CLIST keyword is incorrect when
SEARCH command operates in RACF
subsystem.**

Explanation: AT or ONLYAT was specified along with the CLIST keyword on the SEARCH command. This is not allowed. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued.

System Action: RACF rejects the command.

User Response: Reissue the SEARCH command, either without the CLIST keyword or without either of the following: AT or ONLYAT.

**IRRV020I User ID association retrieval failed
during command direction processing.**

Explanation: RACF processing has determined that a command cannot be directed to the requested user and node because an error occurred while attempting to retrieve user ID association information for the command issuer. This message is accompanied by messages IRRTO03I, IRRTO04I, IRRTO05I, or IRRTO06I, which provide a more detailed analysis of the error. Refer to these messages for further details. This message is sent to the user's TSO terminal.

System Action: The command being processed is unsuccessful; processing ends.

User Response: Verify that the correct command was entered. If it is correct, refer to the message accompanying IRRV020I for more information.

**IRRV021I Command name changed by RACF
installation exit IRREVX01. Command
will not be processed.**

Explanation: The installation command exit, IRREVX01, changed the name of the command issued in the command buffer. This is not allowed.

System Action: Command processing stops. The command return code is set to 12 and the installation exit is called again with a post-processing call to allow processing cleanup to occur.

User Response: Contact your system programmer to report this message.

IRRV022I Command failed by exit. *exit-text*

Explanation: The installation command exit, IRREVX01, has requested that the command fail. The exit can provide additional information in the *exit-text*.

System Action: Command processing stops. The command return code is set to 8 and the installation exit is called again with a post-processing call to allow clean up processing to occur.

User Response: If the *exit-text* does not explain the

cause of the failure, contact your RACF administrator or system programmer.

**IRRV080I RACF command envelope encountered
an error. Abend code is
abend-code-abend-reason-code.**

Explanation: An abend was encountered while attempting to run a RACF command. The command may or may not have run before the abend was encountered. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued, or this message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System Action: Processing is halted at the time of the abend.

User Response: If you were performing an update command (for example, ALTUSER), you may use the appropriate list command (for example, LISTUSER) to determine if the update occurred before the abend. If the problem persists, contact your RACF support personnel and report the problem to the IBM support center. Be sure to indicate the abend code and reason code that were reported in the message.

Problem Determination: Examine the console log and the system abend dump for more information pertaining to the abend.

IRRV098I <internal command buffer>

Explanation: The entire text of this message is an insert. This message is for diagnostic purposes only. It may look different each time it is issued.

The message is issued each time an internal command buffer gets rebuilt. This can be useful when diagnosing command errors. It provides a step-by-step history of how the command text is assembled. These messages are issued only when the RACF subsystem SET command is used to activate the TRACE(IMAGE) option, and a user issues a RACF command that ends in the three characters “-c”. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued.

System Action: The command processes normally even though the command trace was requested.

Problem Determination: You should get these messages only when IBM has asked you to turn on the trace options described above in the “Explanation” section. Save the messages and report them to the IBM support center. Remember to turn off the trace option by using the SET command with the TRACE(NOIMAGE) keyword.

IRRV099I <internal command buffer>

Explanation: The entire text of this message is an insert. This message is for diagnostic purposes only. It may look different each time it is issued.

The message is issued each time an internal command buffer gets rebuilt. This can be useful when diagnosing command errors. It provides a step-by-step history of how the command text is assembled. In addition, this message is used to trace which TSO macros are being used during the parsing of the RACF command. These messages are issued only when the RACF subsystem SET command is used to activate the TRACE(IMAGE) option, and a user issues a RACF command that ends

in the three characters “-t”. This message is sent to the user’s TSO terminal or the operator console, depending on where the command was issued.

System Action: The command processes normally even though the command trace was requested.

Problem Determination: You should get these messages only when IBM has asked you to turn on the trace options described above in the “Explanation” section. Save the messages and report them to the IBM support center. Remember to turn off the trace option by using the SET command with the TRACE(NOIMAGE) keyword.

RRSF operational modes and coupling facility messages

IRRX000I MEMBER *memname* IS IN DATA SHARING MODE.

Explanation: The indicated member is in data sharing mode. RACF will use the coupling facility and will operate in an optimized mode when performing I/O.

System Action: RACF operates in data sharing mode.

Operator Response: None

System Programmer Response: None.

Destination: Descriptor code is 4. Routing code is 2.

IRRX001I IXLREBLD {START | COMPLETE} SERVICE FAILED ON MEMBER *member-name* FOR STRUCTURE *structure-name* CORRESPONDING TO RACF DATABASE *database-name*. IXLREBLD RETURN CODE IS *return-code* AND REASON CODE IS *reason-code*.

Explanation: Member *member-name* was unsuccessful in issuing the IXLREBLD service for the coupling facility structure with return code *return-code* and reason code *reason-code*. Processing may still be successful if another member of the sysplex data sharing group is successful in issuing the IXLREBLD START service.

System Action: A rebuild may still occur for this structure, but not on this system. This system disconnects and enters Read-Only mode.

Operator Response: Save the system console log and notify your system programmer. Refer to the system console for additional messages.

System Programmer Response: Refer to the MVS documentation for further information on IXLREBLD return and reason codes and problem determination.

Destination: Descriptor code is 4. Routing code is 2.

IRRX002I IXLEERSP service failed on member *memname* for structure *strname* corresponding to RACF database *dbname*. IXLEERSP return code is *retcode* and reason code is *rsncode*.

Explanation: Member *memname* was unsuccessful in issuing the IXLEERSP service for the coupling facility structure with return code *retcode* and reason code *rsncode*.

System Action: The member that experienced this error enters or remains in read-only mode and disconnects from the structure *strname*.

Operator Response: Save the system console log and notify your system programmer. Refer to the system console for additional messages.

System Programmer Response: Refer to the MVS documentation for further information on IXLEERSP return and reason codes and problem determination.

Destination: Descriptor code is 4. Routing code is 2.

IRRX003A IXLCONN [REBUILD] SERVICE FAILED TO CONNECT MEMBER *member-name* TO STRUCTURE *structure-name* FOR RACF DATABASE *database-name*. IXLCONN RETURN CODE IS *return-code* AND REASON CODE IS *reason-code*. { REBUILD IS IN PROGRESS }.

Explanation: Member *member-name* was not able to connect to the specified coupling facility structure for the database *database-name*. IXLCONN service failed with the return code *return-code* and reason code *reason-code*.

System Action: The RACF member *member-name* enters or remains in read-only mode. If you receive the message REBUILD IS IN PROGRESS, the connection was conditionally successful but this system disconnects because the structure is being rebuilt by other systems of the sysplex. This allows the rebuild to finish first.

IRRX004I • IRRX010I

Operator Response: Save the system console log and notify your system programmer. Refer to the system console for additional messages.

System Programmer Response: Refer to the MVS documentation for further information on IXLCONN return and reason codes and problem determination.

Destination: Descriptor code is 4. Routing code is 2.

IRRX004I MEMBER *memname* IS IN READ-ONLY MODE.

Explanation: The RACF member *memname* experienced a problem which prevented it from participating in data sharing. The member has automatically entered read-only mode to prevent destroying cache and data coherency of the data sharing group.

System Action: RACF enters read-only mode. Updates to the RACF databases are not allowed from this system.

Operator Response: Notify your system programmer.

System Programmer Response: Refer to the system console for additional error messages and determine the cause of the problem and correct it. For details on CF recovery, see *z/OS Security Server RACF System Programmer's Guide*.

Destination: Descriptor code is 4. Routing code is 2.

IRRX005I MEMBER *memname* IS IN NON-DATA SHARING MODE.

Explanation: The indicated member is in non-data sharing mode. RACF will not use the coupling facility. It will use RESERVE/RELEASE serialization. However, RACF is installed for data sharing and will propagate RVARY and SETROPTS commands.

System Action: RACF operates in non-data sharing mode.

Destination: Descriptor code is 4. Routing code is 2.

IRRX006I MEMBER *memname* EXPERIENCED AN ERROR WHILE PROCESSING THE *command* COMMAND.

Explanation: An error occurred during processing of command *command* for member *memname*. The result of the command on the member *memname* may be unpredictable.

System Action: RACF continues operation.

Operator Response: Save the system console log and notify your system programmer.

System Programmer Response: Examine the console log for the exact nature of the problem and take appropriate action.

Destination: Descriptor code is 4. Routing code is 2.

IRRX008I Rebuild for structure *strname* has been completed.

Explanation: The XES rebuild for structure *strname* has completed across the sysplex.

System Action: This message is presented at the completion of the rebuild regardless of the rebuild's success on the various members in the sysplex. Those members that process the rebuild successfully enter or remain in data sharing mode. If any other error messages are issued in association with this rebuild, those members enter or remain in read-only mode.

Operator Response: If the XES rebuild was not initiated from the console, save the system console log and notify your system programmer. Refer to the system console for additional messages.

System Programmer Response: Refer to the RACF documentation on the related error messages.

Destination: Descriptor code is 4. Routing code is 2.

IRRX009I MEMBER *memname* FAILED {OPEN | READ} FOR RACF DATABASE *dbname*.

Explanation: I/O problems to the RACF database *dbname* have prevented the member *memname* from operating in data sharing mode.

System Action: The system enters or remains in read-only mode.

Operator Response: Notify your system programmer.

System Programmer Response: To recover from this problem, consider switching to a backup RACF database (using the RVARY SWITCH command). For complete information on recovering from this problem, see *z/OS Security Server RACF System Programmer's Guide*. Pay particular attention to the information on failures during I/O operations on the RACF database.

Destination: Descriptor code is 4. Routing code is 2.

IRRX010I MEMBER *memname* COULD NOT ALLOCATE SUFFICIENT STORAGE FOR THE VECTOR TOKEN DURING IXLCONN [REBUILD] OF STRUCTURE *strname*.

Explanation: A severe storage problem, not related to the coupling facility, exists on the system itself. Although the member is connected to the structure, it cannot use the structure, because sufficient storage for the vector token could not be obtained.

System Action: The system enters or remains in read-only mode.

Operator Response: Notify your system programmer.

System Programmer Response: If the lack of

storage cannot be explained or alleviated, contact your z/OS support center. After the storage problem is corrected, either re-IPL the one system or rebuild the structure.

Destination: Descriptor code is 4. Routing code is 2.

IRRX011A STORAGE DEFINED IN POLICY FOR STRUCTURE *strname* IS LESS THAN THE MINIMUM SIZE REQUIRED BY MEMBER *memname* FOR DATABASE *dbname*.

Explanation: The RACF member *memname* is connected to the structure *strname*, but determined that the structure size allocated is less than the minimum storage size required for the database *dbname*.

System Action: The RACF member *memname* enters or remains in read-only mode. RACF remains connected to the structure *strname* in order to allow operator initiated rebuild requests once the policy has been updated.

Operator Response: Notify the system programmer.

System Programmer Response: Correct the policy with sufficient storage for structure *strname*. Refer to *z/OS Security Server RACF System Programmer's Guide* for recommended cache structure sizes and the MVS documentation on managing the coupling facility resource policy. When this is completed, issue a rebuild for the structures to be affected by the policy change.

Destination: Descriptor code is 4. Routing code is 2.

IRRX012I STORAGE ALLOCATED FOR STRUCTURE *strname* IS LESS THAN THE SPECIFIED POLICY SIZE DUE TO COUPLING FACILITY STORAGE CONSTRAINTS.

Explanation: RACF is connected to the indicated structure, but the structure size allocated was less than the size specified by the installation's policy.

Note: This message is always issued if INITSIZE was specified in the STRUCTURE statement.

System Action: RACF remains connected. At least the minimum size required.

- If this message is followed by IRRX013A, the size does not meet the minimum size required. The system enters read-only mode.
- If no other message follows, the size meets the minimum requirements. The system enters data sharing mode.

Operator Response: Notify the system programmer.

System Programmer Response: Reassess and update the coupling facility policy based on available resources. Refer to *z/OS Security Server RACF System Programmer's Guide* for recommended cache structure

sizes and MVS documentation on managing the coupling facility resource policy.

Destination: Descriptor code is 4. Routing code is 2.

IRRX013A STORAGE ALLOCATED FOR STRUCTURE *strname* IS LESS THAN THE MINIMUM SIZE REQUIRED BY MEMBER *memname* FOR DATABASE *dbname*.

Explanation: The RACF member *memname* is connected to the indicated structure, but the structure size allocated was less than the minimum size required for the database *dbname*. This was due to coupling facility storage constraints.

System Action: RACF remains connected to the structure. The system enters or remains in read-only mode.

Operator Response: Notify the system programmer.

System Programmer Response: Reassess and update the coupling facility policy based on available resources. Refer to *z/OS Security Server RACF System Programmer's Guide* for recommended cache structure sizes and MVS documentation on managing the coupling facility resource policy. When this is completed, issue a rebuild for the structures to be affected by the policy change.

If INITSIZE was specified in the STRUCTURE statement, delete it. It causes the size of the structure to be limited to the INITSIZE value instead of the SIZE value.

Destination: Descriptor code is 4. Routing code is 2.

IRRX015A A LINK FAILURE WAS DETECTED BY MEMBER *memname* FOR STRUCTURE *strname* CORRESPONDING TO RACF DATABASE *dbname*.

Explanation: The RACF member *memname* detected a link failure to structure *strname*. The link failure makes this structure inaccessible by this particular member. The database associated with this structure is indicated by *dbname*.

System Action: The member disconnects from the structure and enters or remains in read-only mode.

Operator Response: Refer to the MVS system console for related messages to this link failure. Determine the cause of the link failure and correct the problem. If necessary, contact the IBM support center.

Destination: Descriptor code is 4. Routing code is 2.

IRRX016I **RACF MEMBER *memname* DETECTED A COUPLING FACILITY ERROR DURING function DATABASE NAME = *dbname* XES STRUCTURE NAME = *strname* XES TOKEN = X'aaaa' XES LOCAL CACHE INDEX = X'cccc' RACF RBA = xxxxxxxx XES ERROR CODE = *reason***

Explanation: A coupling facility error was encountered during the processing of either the IXLCACHE or the IXLVECTR service on the indicated member. The function specified will be either IXLVECTR or one of the following IXLCACHE operations: READ, READ OLDNAME, WRITE, WRITE OLDNAME, WRITE ICB, CROSS INVALIDATE, DELETE, DELETE ALL, READ STATS, WRITE WHENREG, or READ NO BUFFER. In the case of a IXLVECTR service failure, the indicated XES Token represents the vector token and the indicated XES Error Code represents the IXLVECTR TESTLOCALCACHE return code. In the case of a IXLCACHE service failure, the indicated XES Token represents the connection token and the indicated XES Error Code represents the IXLCACHE reason code. This information can be used for error analysis by IBM support personnel.

This message will be issued for the first occurrence of an IXLCACHE or IXLVECTR error on the indicated structure. Subsequent errors for the same service on the same structure will not result in this message being issued. Occurrences of the message for that structure will be suppressed until RACF is able to issue a successful invocation of the service. If an error reoccurs after the service has been successfully invoked, the message will be issued again.

System Action: RACF processing continues.

Operator Response: Notify the system programmer.

System Programmer Response: Check for other associated messages. Refer to the MVS documentation for the XES IXLVECTR TESTLOCALCACHE return codes or the IXLCACHE reason codes, which were mentioned in the message.

Destination: Descriptor code is 4. Routing code is 2.

IRRX017I **NO RESPONSE RECEIVED FROM MEMBER *memname* WHILE PROCESSING function.**

Explanation: During processing of the indicated function, a response was not received from the member *memname*.

System Action: RACF will continue to wait for a response from the indicated member. Once a response has been received, RACF will delete this message.

Operator Response: This message might be received if a member is running slower than the coordinator. If this occurs infrequently and this message is deleted, no

action is required. If this message occurs frequently, but is always deleted eventually, contact the IBM support center. If this message is not deleted after a reasonable period of time, notify the system programmer.

System Programmer Response: Examine the console for the exact nature of the problem on member *memname* and correct it. If the problem cannot be corrected, member *memname* must be removed from the sysplex. An IPL will be required.

Destination: Descriptor code is 2. Routing code is 1.

IRRX018I **A COMMUNICATION FAILURE OCCURRED DURING RVARY COMMAND PROPAGATION. MEMBER *memname* CAN NO LONGER USE THE RACF DATABASE.**

Explanation: An XCF communication failure occurred during propagation of an RVARY command. Member *memname* has quiesced activity against the RACF database to process the propagated RVARY command, but is unable to complete processing because of the communication failure. Member *memname* can no longer use the RACF database.

System Action: RACF continues operation, but member *memname* can no longer use the RACF database.

Operator Response: Save the system console log and notify your system programmer.

System Programmer Response: Examine the console log for the exact nature of the XCF failure. Correct the problem and reissue the RVARY command. After member *memname* processes the command, it will be able to use the RACF database again.

Destination: Descriptor code is 4. Routing code is 2.

IRRX020I **REBUILD FOR STRUCTURE *strname* ON MEMBER *memname* HAS BEEN INITIATED.**

Explanation: A rebuild was initiated for a RACF cache structure. This can be caused by one of the following:

- A SETXCF operator command
- A structure failure
- The use of IXLREBLD START by an authorized program
- A loss of connectivity where the coupling facility resource management policy's REBUILDPERCENT *systemweight* value for that structure has been reached.

System Action: RACF participates in the rebuild process. RACF protection remains in effect but the database is unavailable. Processing is suspended for the duration of the rebuild. Message IRRX008I is issued for the same structure name when the rebuild completes.

Operator Response: If the rebuild was not initiated manually via the SETXCF operator command, save the system console log and notify your system programmer. Refer to the system console for additional messages.

Destination: Descriptor code is 4. Routing code is 2.

**IRRX021I REBUILD FOR STRUCTURE *strname*
ON MEMBER *memname* HAS BEEN
STOPPED.**

Explanation: During the XES rebuild, RACF received a rebuild stop signal. This can be caused by one of the following:

- A SETXCF operator command
- The use of IXLREBLD STOP by an authorized program

System Action: RACF disconnects the system from this structure and enters read-only mode.

Operator Response: Save the system console log and notify your system programmer if the stop was not initiated from the console. Refer to the system console for additional messages.

If the system remains in read-only mode, you can use the RVARY DATASHARE command to get RACF to attempt the connections it needs to return to data sharing mode.

Destination: Descriptor code is 4. Routing code is 2.

Chapter 7. IKJ messages

RACF commands were originally TSO commands. (TSO, or Time Sharing Option, is the means by which interactive users gain access to MVS systems.) The RACF commands are treated as TSO commands.

TSO messages (which have a prefix of IKJ) can result from syntax errors made while issuing a RACF command.

For more information on TSO IJK messages, see *z/OS TSO/E Messages*.

Chapter 8. RACF abend codes

This chapter lists and explains the RACF-related abend codes that the system issues to indicate the abnormal completion of a task. Completion codes appear in hexadecimal.

182

Explanation: RACF could not successfully establish an ESTAE recovery environment when processing a RACHECK request.

System Action: The task ends.

Problem Determination: Register 15 contains the nonzero return code passed back from the ESTAE macro. For a description of the ESTAE return code, see *z/OS MVS Programming: Authorized Assembler Services Reference ENF-IXG*.

See *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

Note: For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This ensures that a dump is taken.

183

Explanation: RACF could not successfully establish an ESTAE recovery environment when processing a RACINIT request.

System Action: The task ends.

Problem Determination: Register 15 contains the nonzero return code passed back from the ESTAE macro. For a description of the ESTAE return code, see *z/OS MVS Programming: Authorized Assembler Services Reference ENF-IXG*.

See *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

Note: For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that a dump is taken.

185

Explanation: RACF could not successfully establish an ESTAE recovery environment when processing a RACDEF request.

System Action: The task ends.

Problem Determination: Register 15 contains the nonzero return code passed back from the ESTAE macro. For a description of the ESTAE return code, see the MVS macros and interfaces reference for your system.

See *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

Note: For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that the system produces a dump.

282

Explanation: An error was detected by RACF in the parameters passed to RACF for RACROUTE REQUEST=AUTH processing.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code (message ICH409I, if issued, also contains this reason code):

Code	Explanation
04	Parameter list length not valid.
10	APF authorization, or system key 0-7, or supervisor state required for CSA, LOG, PRIVATE, PROFILE, ACEE, UTOKEN, USERID, or GROUPID option.
14	ATTR option not valid.
18	Volume serial required but not supplied.
1C	Inconsistent PROFILE/ENTITY flag settings.
20	No resource name or PROFILE specified.
24	No CLASS name specified.
2C	Incorrect LOG option specified. (This code is used only through RACF Version 1.4.)
30	Volume serial specified for class other than DATASET.
34	File sequence number not valid.
38	File sequence number specified for non-tape data set.
3C	Tape label parameter specified for non-tape data set.

283

- 40** Tape label option not valid.
- 44** Erase-on-scratch request not valid.
- 48** USERID = * was specified on the REQUEST=AUTH. * is an unacceptable RACF user ID.
- 4C** For the ENTITYX keyword, both the entity name length and the buffer length are zero.
- 50** Buffer length is not valid:
- Less than zero
 - Greater than 255
 - Not zero but less than the entity name length.
- 54** Entity name length is not valid:
- Less than zero
 - Greater than 44 if CLASS=DATASET, or greater than the length for that class as defined in the class-descriptor table
 - Greater than 44 if CLASS=DATASET, or greater than the maximum length for that class as defined in the class-descriptor table.
- 58** The in-storage profile provided to the REQUEST=AUTH was not at the version required by RACF. Ensure that the version of the in-storage profile (addressed by the ENTITY parameter with CSA specified) is at the required version number.
- 5C** The entity name contains a blank.
- If the ENTITYX keyword is specified and the entity name length is given, the name has a blank in the beginning, in the middle, or at the end.
- 60** RTOKEN keyword is mutually exclusive with the CSA and PRIVATE parameters of the ENTITY keyword.
- 64** ACEE not valid.
- 68** Unauthorized caller specified subpool greater than 127 on RACROUTE MSGSP parameter.
- 6C** The message chain pointed to by SAFPMASD for an unauthorized caller contains too many elements, indicating a chaining problem.

Identify and correct the indicated error.

Problem Determination: Use the reason code in Register 15 to identify the error. If the issuer of the RACF macro is a user routine (such as an installation exit), correct the parameter list specified for the RACF macro in the installation exit. If the issuer of the RACF macro is an IBM routine, see *z/OS Security Server RACF Diagnosis Guide* for more information on diagnosing abends and reporting abend problems to IBM.

Note: For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This ensures that a dump is taken.

283

Explanation: An error was detected by RACF in the parameters passed to RACF for RACROUTE REQUEST=VERIFY processing.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code	Explanation
04	Incorrect parameter list length.
14	ENVIR data specified was not valid.
18	USERID specified did not conform to length requirements.
1C	PASSWRD specified did not conform to length requirements.
20	GROUP specified did not conform to length requirements.
24	NEWPASS specified did not conform to length requirements.
28	OIDCARD specified had length field=0.
30	Incorrect combination of ENVIR keyword data and USERID, PASSWRD, NEWPASS, START, OIDCARD, TERMID, APPL SESSION, TRUSTED, REMOTE, SECLABEL, EXENODE, SUSERID, SNODE, SGROUP, POE, TOKNIN, and STOKEN specified.
34	Incorrect combination of ENVIR keyword data and GROUP specified.
38	ENVIR = CHANGE specified but no ACEE exits.
40	Reserved
44	ENVIR=CREATE and SESSION=APPCTP were specified but POE was not specified and is required in this case.
48	ENVIR=CREATE and SESSION=APPCTP were specified but APPL was not specified and is required in this case.
4C	The ACEE specified does not appear to be a valid ACEE.
50	The ENVRIN keyword was specified and the ENVR object storage area address was zero, or, either the ENVRIN or ENVROUT keyword

- was specified and the ENVR object storage area was not on a doubleword boundary.
- 54** The ENVRIN keyword was specified and the ENVR object contained in the ENVR object storage area was larger than the ENVR object storage area specified.
- This can be caused by using an ENVR object from another external security manager. For example, MCS console services routes commands from other systems with ENVRIN data.
- 58** The X500NAME keyword supplied an X500 name pair data structure as indicated by a non-zero structure length, but either the length of the issuer's name or the length of the subject's name is not in the correct range (1 to 255).

Identify and correct the indicated error.

Problem Determination: Use the reason code in Register 15 to identify the error. If the issuer of the RACF macro is a user routine (such as an installation exit), correct the parameter list specified for the RACF macro in the installation exit. If the issuer of the RACF macro is an IBM routine, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

Note: For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that a dump is taken.

285

Explanation: RACF detected an error in the parameters passed to it for RACDEF request processing.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code Explanation

- 04** Parameter list length is not valid.
- 08** Level number is not valid.
- 0C** TYPE option is not valid.
- 10** Resource name required. *Entity-name* (and *newname* keywords, if specified) must point to valid, non-blank resource names.
- 14** New data set name or old volume serial specified but address is zero.
- 18** Volume serial required but not specified.

- 1C** New data set name and old volume serial flags both set.
- 24** Parameters supplied which are inconsistent for a general resource class other than DATASET. These incorrect parameters might be model name, model volume serial, VSAM data set bit on, old volume serial, or new data set name.
- 28** Model resource information supplied with type other than DEFINE for DATASET class.
- 2C** Model name supplied but model volume serial not supplied.
- 30** Unqualified data set name specified. This return code is not issued if RACFIND=NO was specified.
- 34** Old volume serial number is absent for CHGVOL request.
- 38** Length of the unit field is not valid.
- 3C** AUDIT value is not valid.
- 40** Specified OWNER is not valid. This reason code can occur for several reasons. Among the possible reasons are:
- The OWNER is not a RACF-defined user ID or group ID.
 - The OWNER is a RACF-defined user ID but that user ID is revoked.
- 44** UACC value is not valid.
- 48** Rename request is not valid. Either ENTITY name or NEWNAME name, but not both, is a generic name. This reason code could occur because of the attempt to create a data set profile with a single-qualifier name, when RACF protection for single-qualifier names has not been activated (SETROPTS command with PREFIX specified). Note that there are several cases in which data set profiles can be created automatically: when users with the ADSP attribute create data sets, when PROTECT=YES is specified in JCL, and when a user issues the ADDSD command.
- 4C** Type=CHGVOL specified for TAPE.
- 50** Parameters specified for TAPE are not valid.
- 54** FILESEQ omitted when required for TAPE.
- 58** Operands specified for DASD are not valid.
- 5A** The in-storage profile provided to the RACHECK request was not at the version required by RACF. Ensure that the version of the in-storage profile (addressed by the ENTITY parameter with CSA specified) is at the required version number.
- 5C** FILESEQ value is not valid.
- 60** TAPELBL value is not valid.

64	EXPDT/RETPD value is not valid.		
68	NOTIFY user ID is not valid.		
6C	RESOWNER specified for other than TYPE=DEFINE.		
70	Specified RESOWNER is not valid.		
74	MGMTCLAS and/or STORCLAS specified without RESOWNER.		
78	Length for MGMTCLAS is not valid.		
7C	Length for STORCLAS is not valid.		
80	Length for RESOWNER is not valid.		
84	Specified SECLABEL is not valid.		
88	Buffer length specified with ENTITYX keyword is not valid: <ul style="list-style-type: none"> • Less than zero • Greater than 255 • Not zero but less than the entity name length 		
8C	Name length specified with ENTITYX keyword is not valid. <ul style="list-style-type: none"> • The specified length is less than zero. • The specified length is greater than 44 if CLASS=DATASET or greater than the maximum length for that class as defined in the class-descriptor table. • The name which was supplied is longer than 44 if CLASS=DATASET or longer than the maximum length for that class as defined in the class-descriptor table. 		
90	For the ENTITYX format, both the entity name length and the buffer length are zero.		
94	Buffer length specified with MENTX keyword is not valid: <ul style="list-style-type: none"> • Less than zero • Greater than 255 • Not zero but less than the entity name length 		
98	Name length specified with MENTX keyword is not valid: <ul style="list-style-type: none"> • The specified length is less than zero. • The specified length is greater than 44 if CLASS=DATASET or greater than the maximum length for that class as defined in the class-descriptor table. 		
9C	For the MENTX keyword, both the entity name length and the buffer lengths are zero.		
A0	Buffer length specified with NEWNAMX keyword is not valid: <ul style="list-style-type: none"> • Less than zero • Greater than 255 		
			<ul style="list-style-type: none"> • Not zero but less than the entity name length.
		A4	Name length specified with NEWNAMX keyword is not valid: <ul style="list-style-type: none"> • The specified length is less than zero. • The specified length is greater than 44 if CLASS=DATASET or greater than the maximum length for that class as defined in the class-descriptor table. • The name that was supplied is longer than 44 if CLASS=DATASET or longer than the maximum length for that class as defined in the class-descriptor table.
		A8	For the NEWNAMX keyword, both the entity name length and the buffer lengths are zero.
		AC	The profile name for the FILE and DIRECTRY class does not contain at least two valid qualifiers for keyword ENTITY or ENTITYX. <ul style="list-style-type: none"> • The profile name contains only one qualifier. • The profile name begins with a period. • The second qualifier is longer than 8 characters.
		B0	The profile name for the FILE and DIRECTRY class does not contain at least two valid qualifiers for keyword MENTY or MENTX. <ul style="list-style-type: none"> • The profile name contains only one qualifier. • The profile name begins with a period. • The second qualifier is longer than 8 characters.
		B4	The profile name for the FILE and DIRECTRY class does not contain at least two valid qualifiers for keyword NEWNAME or NEWNAMX. <ul style="list-style-type: none"> • The profile name contains only one qualifier. • The profile name begins with a period. • The second qualifier is longer than 8 characters.
		B8	The entity name contains a blank: If the ENTITYX keyword is specified and the entity name length is given, the name has a blank in the beginning, in the middle, or at the end.
		BC	The model profile name contains a blank. If the MENTX keyword is specified and the name length is given, the name has a blank in the beginning, in the middle, or at the end.
		C0	The new profile name contains a blank. If the NEWNAME keyword is specified and the new name length is given, the name has a blank in the beginning, in the middle, or at the end.

- C8** Specified SECLVL is not valid:
- The number of data fields is not zero or one.
 - The value of the data fields is not within the range of 1 - 254.

Identify and correct the indicated error.

Problem Determination: Use the reason code in Register 15 to identify the error. If the issuer of the RACF macro is a user routine (such as an installation exit), correct the parameter list specified for the RACF macro in the installation exit. If the issuer of the RACF macro is an IBM routine, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

Note: For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that a dump is taken.

382

Explanation: The RACROUTE REQUEST=AUTH preprocessing or postprocessing exit routine passed an incorrect return code to RACF. The return code was not part of the defined interface.

System Action: The task ends.

Programmer Response: Possible user error. Register 15 contains the return code from the exit routine. Verify that the exit routine is issuing valid return codes. See *z/OS Security Server RACROUTE Macro Reference* for the correct return codes.

Problem Determination: If the installation exit is issuing a correct return code and RACF still issues this abend, call your IBM support center for advice about whether this is a documentation error or an incorrect output error. See *z/OS Security Server RACF Diagnosis Guide* for information on reporting documentation errors or incorrect output to IBM.

Note: Before calling IBM, make sure the return code passed by the installation exit is correct.

383

Explanation: The RACROUTE REQUEST=VERIFY preprocessing or postprocessing exit routine passed an incorrect return code to RACF. The return code was not part of the defined interface.

System Action: The task ends.

Programmer Response: Possible user error. Register 15 contains the return code from the exit routine. Verify that the exit routine is issuing valid return codes. See *z/OS Security Server RACROUTE Macro Reference* for the correct return codes.

Problem Determination: If the installation exit is issuing a correct return code and RACF still issues this abend, call your IBM support center for advice about whether this is a documentation error or an incorrect output error. See *z/OS Security Server RACF Diagnosis Guide* for information on reporting documentation errors or incorrect output to IBM.

Note: Before calling IBM, make sure the return code passed by the installation exit is correct.

383

Explanation: The RACROUTE REQUEST=VERIFY preprocessing or postprocessing exit routine passed an incorrect return code to RACF. The return code was not part of the defined interface.

System Action: The task ends.

Programmer Response: Possible user error. Register 15 contains the return code from the exit routine. Verify that the exit routine is issuing valid return codes. See *z/OS Security Server RACROUTE Macro Reference* for the correct return codes.

Problem Determination: If the installation exit is issuing a correct return code and RACF still issues this abend, call your IBM support center for advice about whether this is a documentation error or an incorrect output error. See *z/OS Security Server RACF Diagnosis Guide* for information on reporting documentation errors or incorrect output to IBM.

Note: Before calling IBM, make sure the return code passed by the installation exit is correct.

385

Explanation: The RACROUTE REQUEST=VERIFY preprocessing or postprocessing exit routine passed an incorrect return code to RACF. The return code was not part of the defined interface.

System Action: The task ends.

Programmer Response: Possible user error. Register 15 contains the return code from the exit routine. Verify that the exit routine is issuing using valid return codes. See *z/OS Security Server RACROUTE Macro Reference* for the correct return codes.

Problem Determination: If the installation exit is issuing a correct return code and RACF still issues this abend, call your IBM support center for advice about whether this is a documentation error or an incorrect output error. See *z/OS Security Server RACF Diagnosis Guide* for information on reporting documentation errors or incorrect output to IBM.

Note: Before calling IBM, make sure the return code passed by the installation exit is correct.

3C7

Explanation: While RACF was processing a non-SVC request, an error occurred in the RACF storage manager.

System Action: The system terminates the service request.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code	Explanation
------	-------------

04	BAD LENGTH: The length of the area to get or free is not greater than zero.
08	BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C	DUPLICATE FREEMAIN: The area to free has already been freed.
10	INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14	INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18	NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.
1C	FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.
20	NOT FREED: There is a temporary area still allocated at the end of processing.
A0	A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.
A4	A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.
A8	A RACF module issued a free-space request. However, register 1 is equal to zero.
AC	A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see *z/OS Security Server RACF Diagnosis Guide*.

482

Explanation: While RACF was processing a RACHECK request, the RACF manager returned an return code that was not valid.

System Action: The system stops the task.

Programmer Response: Register 15 contains the hexadecimal return code from the RACF manager, but Register 0 does not contain the RACF manager reason code. (Message ICH409I, if issued, contains this reason code.) See "RACF Manager Return Codes" on page 307 for an explanation of RACF-manager return codes.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see *z/OS Security Server RACF Diagnosis Guide*.

483

Explanation: While RACF was processing a RACINIT request, the RACF manager returned an incorrect return code.

System Action: The task ends.

Programmer Response: Register 15 contains the return code from the RACF manager, but Register 0 will not contain the RACF manager reason code. See "RACF Manager Return Codes" on page 307 for an explanation of RACF-manager return codes.

Problem Determination: If a dump was taken for this abend, use IPCS, to format the dump. For an explanation of the dump title, see the dump title beginning **ICHRST00-RACF SVCS** in *z/OS Security Server RACF Diagnosis Guide*.

485

Explanation: While RACF was processing a RACROUTE REQUEST=DEFINE request, the RACF manager returned an incorrect return code.

System Action: The task ends.

Programmer Response: Register 15 contains the return code from the RACF manager, but Register 0 will not contain the RACF manager reason code. See "RACF Manager Return Codes" on page 307 for an explanation for RACF-manager return codes.

Problem Determination: If a dump was taken for this abend, use IPCS, to format the dump. For an explanation of the dump title, see the dump title beginning **ICHRST00-RACF SVCS** in *z/OS Security Server RACF Diagnosis Guide*.

4C6

Explanation: An error occurred because the required control blocks were not present when a callable security service was processed. A hexadecimal reason code in register 15 describes the error. See the reason code for a description of the error.

System Action: The system abnormally ends the task.

Programmer Response: RACF input/output parameter list IRRPCOMP contains a SAF return code, RACF return code, and RACF reason code that describes an internal RACF error. For additional information on the parameter list IRRPCOMP, see *z/OS Security Server RACF Callable Services*.

Code (hex)**Explanation**

- | | |
|-----------|---|
| 04 | A service call to a RACF module was not completed. No accessor environment element (ACEE) was available to describe the error. |
| 08 | A service call to a RACF module was not completed. No accessor environment element extension (ACEX) was available to describe the user. |
| 0C | A service call to a RACF module was not completed. No user security packet (USP) was available to describe the user. |

System Programmer Response: Run the job again or have the user log on again while RACF is active. If the abend occurs again, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

4C7

Explanation: While RACF was processing a non-SVC request, an error occurred in the RACF storage manager.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code Explanation

- | | |
|-----------|--|
| 04 | BAD LENGTH: The length of the area to get or free is not greater than zero. |
| 08 | BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary. |
| 0C | DUPLICATE FREEMAIN: The area to free has already been freed. |
| 10 | INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated. |
| 14 | INVALID OVERLAP: Part of the area to free |

equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.

- | | |
|-----------|--|
| 18 | NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have. |
| 1C | FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have. |
| 20 | NOT FREED: There is a temporary area still allocated at the end of processing. |
| A0 | A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program. |
| A4 | A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated. |
| A8 | A RACF module issued a free-space request. However, register 1 is equal to zero. |
| AC | A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program. |

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see *z/OS Security Server RACF Diagnosis Guide*. Look at the messages in the job log for the name of the module calling RACF. For modules supplied by IBM, search problem reporting databases for a fix for the problem. If no fix exists, contact the IBM support center.

582

Explanation: While processing a RACROUTE REQUEST=AUTH request, RACF was unable to verify a user.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. Message ICH409I, if issued, also contains this return code.

Code Explanation

- | | |
|--|--|
| 00 | No accessor control environment (ACEE) was available to describe the user. |
| Note: This is normal if a job started or a user logged on while RACF was inactive but has since been reactivated. | |
| 04 | Reserved. |

Identify and correct the indicated error.

Problem Determination: Run the job again, or have the user log on again while RACF is active. If the abend occurs again, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

585

Explanation: While processing a RACROUTE REQUEST=DEFINE request, RACF encountered an error.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this return code.)

Code Explanation

00 No accessor environment element (ACEE) was available to describe the user.

Note: This is normal if a job started or a user logged on while RACF was inactive but has since been reactivated.

04 No UCB was found to contain a volume serial that matched the volume serial passed to RACF in the REQUEST=DEFINE macro instruction for a TYPE=DEFINE operation.

08 The ADDVOL or CHGVOL function was requested but the user did not have at least UPDATE authority to the data set.

0C The ADDVOL function was requested and (1) the volume serial number is already defined (for DATASET class), or (2) the new tape volume is already defined (for TAPEVOL class).

The CHGVOL function was requested and a data set profile with ENTITY name and a new volume serial number is already defined.

Identify and correct the indicated error.

Problem Determination: For reason code 00, run the job again, or have the user log on again while RACF is active. If the abend occurs again, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM. For the other reason codes, correct the problem indicated by the reason code. For assistance in gathering additional information about the request that caused this abend (such as obtaining a dump or identifying the caller of RACF), see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends. If an IBM program issued the REQUEST=DEFINE macro, see *z/OS Security Server RACF Diagnosis Guide* for information on reporting abend problems to IBM.

683

Explanation: The module calling RACROUTE REQUEST=VERIFY is not authorized (is not APF-authorized, in system key 0-7, or in supervisor state).

Note: If the NEWPASS keyword is not specified on the REQUEST=VERIFY, you can authorize the calling module by entering it in the RACF-authorized caller table. However, IBM does not recommend placing entries in the RACF-authorized caller table.

System Action: The task is terminated.

Programmer Response: Possible user error. Verify that the module is an authorized caller.

Problem Determination: If the request originated as a RACF command (that in turn resulted in the issuing of the REQUEST=VERIFY), check to make sure the RACF command is in the list of APF-authorized commands for your system.

If the module making the request is an IBM routine, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

684

Explanation: The module calling the RACF manager or the RACROUTE REQUEST=LIST or RACROUTE REQUEST=EXTRACT function is not authorized (is not APF-authorized, in system key 0-7, or in supervisor state).

Note: If the NEWPASS keyword is not specified on the REQUEST=VERIFY, you can authorize the calling module by entering it in the RACF-authorized caller table. However, IBM does not recommend placing entries in the RACF-authorized caller table.

System Action: The task ends.

Programmer Response: Possible user error. Verify that the module is an authorized caller.

Problem Determination: If the request originated as a RACF command (that in turn resulted in a call to the RACF manager or the REQUEST=LIST), check to make sure the RACF command is in the list of APF-authorized commands for your system.

If the module making the request is an IBM routine, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

685

Explanation: The module calling RACROUTE REQUEST=DEFINE is not authorized (is not APF-authorized, in system key 0-7, or in supervisor state). To issue a REQUEST=DEFINE, the calling module must be authorized (APF-authorized, in system key 0-7, or in supervisor state).

System Action: The task ends.

Programmer Response: Possible user error. Verify that the calling module was executing in an authorized state.

Problem Determination: If the request originated as a RACF command (that in turn resulted in the issuing of the REQUEST=DEFINE), check to make sure the RACF command is in the list of APF-authorized commands for your system.

If the module making the request is an IBM routine, see *z/OS Security Server RACF Diagnosis Guide* for information on diagnosing abends and reporting abend problems to IBM.

9C7

Explanation: RACROUTE functions dealing with tokens (such as VERIFY, VERIFYX, TOKENBLD, TOKENMAP) will issue an abend 9C7 when an incorrect token is detected.

System Action: The task ends.

Programmer Response: This is possibly a user error. Verify that the token interface is correct.

Problem Determination: Check the reason code and make sure you pass the correct token in the request.

The following reason codes will be issued with abend 9C7.

Code	Explanation
01	STOKEN area is too small.
02	TOKNIN area is too small.
04	The request is TOKENMAP. TOKNIN is a required parameter. Either it was not specified or both its length and version fields are 0.
08	The request is VERIFYX, TOKENBLD, TOKENMAP, or TOKENXTR. TOKNOUT is a required parameter. Either it was not specified or both its length and version fields are 0.
0C	Version of 0 can only be used in conjunction with a length of 0, as an alternate method of <i>not</i> specifying a token parameter. This token is not valid because the token's version is 0 but its length is not.
10	VERSION=0.
14	USERID has length greater than 8 characters.

18	PASSWORD has length greater than 8 characters.
1C	GROUPID has length greater than 8 characters.
20	NEWPASSWORD has length greater than 8 characters.
24	EXENOSDE has length greater than 8 characters.
28	SUSERID has length greater than 8 characters.
2C	SNODE has length greater than 8 characters.
30	SGROUP has length greater than 8 characters.
34	TOKNOUT version is greater than the current maximum.

AC5

Explanation: An unexpected error was encountered during internal RACF processing for datasharing or sysplex communication functions. A hexadecimal reason code is given in register 15.

System Action: A dump will be taken in all cases. If the abend occurs in the RACF data sharing address space, the address space will be restarted. If the abend occurs in the master address space, the system will enter failsoft mode.

Programmer Response: the abend occurred in the master address space, the system will need to be re-IPLed in order for RACF to be made active again. If necessary, contact your programming support personnel.

Code	Explanation
03	An error occurred when attempting to obtain storage.
05	An error occurred when attempting to free storage.
07	After IXCJOIN, all other members left the data sharing group before the group data set name and range table were received. One reason this can happen is that you are IPLing a system and all other systems in the group were simultaneously re-IPLed. If this is the case, re-IPL your system. Otherwise, contact the IBM support center.
08	An XCF service failed during sysplex communication.
0F	XCF services failed. RACF will try to restart the RACF datasharing address space.
10	This abend occurs when a system in datasharing mode is put into failsoft mode due to the occurrence of some other error.

D82 • D83

nn An internal RACF error has occurred. Contact the IBM support center.

D82

Explanation: While RACF was processing a RACROUTE REQUEST=AUTH, an error occurred in the RACF storage manager.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code	Explanation
04	BAD LENGTH: The length of the area to get or free is not greater than zero.
08	BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C	DUPLICATE FREEMAIN: The area to free has already been freed.
10	INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14	INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18	NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.
1C	FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.
20	NOT FREED: There is a temporary area still allocated at the end of SVC processing.
A0	A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.
A4	A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.
A8	A RACF module issued a free-space request. However, register 1 is equal to zero.
AC	A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the

dump title, see *z/OS Security Server RACF Diagnosis Guide*.

D83

Explanation: While RACF was processing a RACROUTE REQUEST=VERIFY, an error occurred in the RACF storage manager.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code	Explanation
04	BAD LENGTH: The length of the area to get or free is not greater than zero.
08	BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C	DUPLICATE FREEMAIN: The area to free has already been freed.
10	INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14	INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18	NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.
1C	FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.
20	NOT FREED: There is a temporary area still allocated at the end of SVC processing.
A0	A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.
A4	A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.
A8	A RACF module issued a free-space request. However, register 1 is equal to zero.
AC	A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the

dump title, see *z/OS Security Server RACF Diagnosis Guide*.

D84

Explanation: While RACF was processing a RACROUTE REQUEST=LIST, an error occurred in the RACF storage manager.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code	Explanation
04	BAD LENGTH: The length of the area to get or free is not greater than zero.
08	BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C	DUPLICATE FREEMAIN: The area to free has already been freed.
10	INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14	INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18	NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.
1C	FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.
20	NOT FREED: There is a temporary area still allocated at the end of SVC processing.
44	Too many actions specified on ICHEINTY macro.
A0	A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.
A4	A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.
A8	A RACF module issued a free-space request. However, register 1 is equal to zero.
AC	A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see *z/OS Security Server RACF Diagnosis Guide*.

D85

Explanation: While RACF was processing a RACROUTE REQUEST=DEFINE, an error occurred in the RACF storage manager.

System Action: The task ends.

Programmer Response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code	Explanation
04	BAD LENGTH: The length of the area to get or free is not greater than zero.
08	BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C	DUPLICATE FREEMAIN: The area to free has already been freed.
10	INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14	INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18	NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.
1C	FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.
20	NOT FREED: There is a temporary area still allocated at the end of SVC processing.
A0	A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.
A4	A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.
A8	A RACF module issued a free-space request. However, register 1 is equal to zero.
AC	A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

E82 • E85

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see *z/OS Security Server RACF Diagnosis Guide*.

E82

Explanation: SVC 130 (RACROUTE REQUEST=AUTH macro) was invoked; however, SVC 130 is inactive because RACF is not properly installed on the system.

System Action: The task stops.

Programmer Response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.

If you have not installed RACF on your system, this abend could be issued when a data set has the RACF indicator bit on. This could occur if the data set came from a system with RACF installed.

E83

Explanation: SVC 131 (RACROUTE REQUEST=VERIFY macro) was invoked; however, SVC 131 is inactive because RACF is not properly installed on the system.

System Action: The task stops.

Programmer Response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.

E84

Explanation: SVC 132 (RACROUTE REQUEST=LIST macro) was invoked; however, SVC 132 is inactive because RACF is not properly installed on the system.

System Action: The task stops.

Programmer Response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your

IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.

E85

Explanation: SVC 133 (RACROUTE REQUEST=DEFINE macro) was invoked; however, SVC 133 is inactive because RACF is not properly installed on the system.

System Action: The task stops.

Programmer Response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.

Chapter 9. RACF return codes

This section lists and explains return codes for:

- RACF manager
- RACF utilities

RACF Manager Return Codes

This section lists and explains the RACF manager return codes. It contains Programming Interfaces that allow you to write programs to obtain the services of the OS/390 Security Server.

The RACF manager returns the codes to the caller (a RACF SVC, a command processor, or a user-written program) in hexadecimal in Register 15.

Code	Explanation
------	-------------

Hex (Decimal)	
---------------	--

0 (0)	The requested operation was successful.
-------	---

4 (4)	A recovery environment could not be established.
-------	--

8 (8)	An attempt was made to add an entry (a profile) to the RACF database but an identical entry already exists.
-------	---

Note: Identical entries have the same name, type, and (if specified) volume.

C (12)	For requests other than NEXT or NEXTC, the specified entry (RACF profile) did not exist. For NEXT or NEXTC requests, no subsequent entries (RACF profiles) satisfied the request.
--------	--

10 (16)	Reserved.
---------	-----------

14 (20)	The RACF database did not contain enough space to satisfy the request.
---------	--

18 (24)	An I/O error occurred while accessing the RACF database. The RACF manager uses the EXCP macro to access the RACF database. This error could be caused by a problem with the DASD on which the RACF database is stored.
---------	--

1C (28)	RACF was not active at the time of the request; or, in an environment with multiple RACF data sets, the RACF data set containing the requested profile is inactive.
---------	---

19 (25)	The number of actual tests for the ICHEINTY request for the CONNECT type profile is more than 254.
---------	--

20 (32)	One of the following occurred:
---------	--------------------------------

1. The request type requires a user work area but the area was not provided (the address in the parameter list was 0).
2. For a RENAME, neither NEWNAME nor NEWNAMEX was supplied.

24 (36)	The input parameter list or the associated ACTION and TEST blocks contain an error. For abend 482, 483, or 485, this RACF manager return code usually indicates that down-level templates are being used for the RACF database. Template conversion is done with IRRMIN00. Do the following:
---------	--

1. Check the output of IRRMIN00 to be sure higher-level templates were used.
2. Check that the higher level of IRRMIN00 was run.
3. Check that IRRMIN00 was run against the correct RACF data base. RACF uses the templates from the first primary RACF database activated.

4. Check that an unconverted database was not copied over the one that had IRRMIN00 run against it.

When this code is returned, register 0 contains one of the following reason codes:

Code	Explanation
Hex (Decimal)	
1 (1)	Entry name (profile name) or NEWNAME is not valid.
2 (2)	Action(s) specified with DELETE or DELETEA.
3 (3)	An action specified for an undefined field.
4 (4)	Test(s) specified with RENAME.
5 (5)	Reserved.
6 (6)	Reserved.
7 (7)	Incorrect entry type (profile type).
8 (8)	DATAMAP(OLD) was coded on the ICHEINTY macro, and GROUP=YES was coded on the ICHEACTN macro, but the given data length was too long for the repeat group.
9 (9)	DATAMAP(OLD) was coded on the ICHEINTY macro, and GROUP=YES was coded on the ICHEACTN macro, but the given data length was too short for the repeat group.
A (10)	Consistency error between multiple input parameter lists. This error occurs if chaining is being used and all input parameter lists are not using the same options or the same values for: TYPE, RBA, CLASS, VOLID, ENTRY, SMC, GENERIC or INDEX.
B (11)	Input parameter list chaining/request type combination error. This error occurs when the rules for types of input parameter list requests that may be chained are violated. For example, the first input parameter list can only be a NEXT or NEXTC, LOCATE, ALTER or ALTERI, DELETE with SEGMENT or ADD. The following input parameter lists can only be LOCATE (after LOCATE), NEXT/NEXTC (after NEXT/NEXTC), ALTERI (after ALTERI), ALTER (after ALTER, DELETE or ADD), and DELETE with SEGMENT (after ALTER or DELETE).
C (12)	All input parameter lists specify RUN=NO.
D (13)	Request type/segmentation combination error. This error occurs if a segment name is specified with ADD, DELETEA, or RENAME.
E (14)	Invalid field for GROUP=YES. This error occurs if GROUP=YES was coded but the field is not a repeat group.
F (15)	Input parameter list limit exceeded. More than 1000 input parameter lists were chained.
10(16)	Segment not allowed. Specified SEGMENT name not allowed for the specified profile TYPE.
11(17)	Inconsistency between ACTION data length and repeat group FIELDS, GROUP=YES. This is similar to return code 8, but DATAMAP(NEW) was coded on the ICHEINTY macro.
12 (18)	Data length specified on ICHEACTN macro exceeded the length of the specified fixed-length field.

13 (19)	Inconsistency between action data length and repeat group fields. GROUP=YES data is too short.
14 (20)	Invalid ENTRYX. Current length is greater than 44 and either the primary or the backup database is not in the restructured (RDS) format.
15 (21)	Invalid NEWNAMX. Current length is greater than 44 and either the primary or the backup database is not in the restructured (RDS) format.
16 (22)	Data length specified on the ICHEACTN macro was less than zero and neither FLDATA='DEL' nor FLDATA='COUNT' was specified.
17 (23)	The generic entity name exceeds the maximum length after it has been encoded.
18 (24)	Limit has been reached for the concurrent source request.
19 (25)	Number of tests is greater than 254.
1A (26)	Invalid date supplied on an ICHEACTN when DATEFMT=YYYYDDDF is specified.
1B (27)	Repeat count cannot be updated when GROUP=NO is specified.
1C (28)	Alias locate requested but database is stage 0 or 1.
1D (29)	Alias processing not supported for request type.
1E (30)	Alias locate requested for a non-alias field.
1F (31)	Base pointer for test is 0 on an alias locate request.
20 (32)	Alias name length is 0 or greater than 252.
28 (40)	The maximum profile size (65,535 bytes) has been reached; the profile cannot be expanded.
2C (44)	The user-supplied work area was not large enough to hold all the data returned. The work area is filled with data up to, but not including, the first field that did not fit.
30 (48)	The user-supplied work area was smaller than the minimum amount required (30 bytes).
34 (52)	A test condition specified in the TESTS keyword of the ICHEINTY macro was not met; RACF stopped processing.
38 (56)	You requested an operation on an entry (profile) in class DATASET that has multiple RACF definitions, but you did not specify a VOLUME to single out a specific entry.
3C (60)	For DATASET class entries, you specified a VOLUME that did not exist in the volume list of any entry with the specified name. For TAPEVOL class entries, a request tried to add a new TAPEVOL to a nonexistent tape volume set.
40 (64)	You attempted to delete one of the IBM-defined entries (such as SYS1 or IBMUSER) from the RACF database.
44 (68)	An ALTERI request attempted to increase the size of the profile being updated.
48 (72)	A request to add an entry to the RACF database would have caused the RACF index to increase to a depth that RACF does not support (the maximum depth is 10 levels).
4C (76)	ICHEINTY encountered an invalid index block or read a non-index block when it expected an index block.
50 (80)	An attempt was made to update one of the following (by a request other than ALTERI): <ul style="list-style-type: none"> • The RACF database that has been locked by a RACF utility • The RACF database from a system that is in read-only mode (in a RACF sysplex data sharing environment)

54 (84)	Reserved (used internal to RACF).
58 (88)	Some field-level access checks failed for data retrieval.
5C (92)	All field-level access checks failed for data retrieval.
60 (96)	Field-level access checks failed for data update.
64 (100)	Reserved for use by the ICHEINTY macro for RELEASE=(xx,CHECK).
68 (104)	Invalid data in a RACF profile. Detail code is in the reason code:
Code Explanation Hex (Decimal)	
	1 (1) Profile too short
6C (108)	The RACF manager has been invoked recursively, and an exclusive reserve/enqueue is required. However a shared reserve/enqueue is already held.
70 (112)	The RACF manager received an unexpected return code from a reserve/enqueue. The reserve/enqueue return code is passed back in register 0.
78 (120)	Reserved (used internal to RACF).
7C (124)	Reserved (used internal to RACF).
80 (128)	This is a data sharing mode return code. A coupling facility function had a problem when dealing with the ICB.
84 (132)	Maximum alias index entry size has been reached.

RACF Utilities Return Codes

This section describes the return codes for the RACF utilities. This information is also described in *z/OS Security Server RACF System Programmer's Guide* for the programmer creating jobs that use the utility.

Table 1. Return Codes for the IRRUT100 Utility

Hex (Decimal)	Explanation
0 (0)	Function successful. Report printed.
4 (4)	Insufficient authority. See your RACF security administrator.
8 (8)	Error. Report not printed.
10 (16)	Open of SYSPRINT DCB failed.
20 (32)	RACF is not enabled. Process ends.

Table 2. Return Codes for the IRRUT200 Utility

Hex (Decimal)	Explanation
0 (0)	Function successful. Report printed.
4 (4)	A noncritical error was detected. Report printed.
8 (8)	A critical error was detected. Utility processing may not have completed. Any report printed may not be complete.
C (12)	Utility terminated because: <ul style="list-style-type: none"> • A request for storage failed. • The ICB (inventory control block) or top-level index block could not be read (or was invalid). • The utility was unable to open a required data set. • The database (SYSRACF) and work data set (SYSUT1) device types have incompatible track geometries.
20 (32)	RACF is not enabled. Process ends.

Table 3. Return Codes for the IRRUT400 Utility

Hex (Decimal)	Explanation
0 (0)	Successful completion without error.
4 (4)	Duplicate IBM-defined names caused one or more warning conditions.
8 (8)	One or more error conditions occurred because of one of the following reasons: <ul style="list-style-type: none"> • Duplicate non-IBM-defined names. • A defective tape volume set.
C (12)	One or more severe error conditions resulted from an error on an output database.
10 (16)	A terminating error condition occurred because of one of the following reasons: <ul style="list-style-type: none"> • A recovery environment could not be established. • The SYSPRINT file could not be opened. • An error was found in a parameter specification. • A range table was requested but could not be loaded. • An error was detected in the specified range table. • An error occurred on an input database.
20 (32)	RACF is not enabled. Process ends.

Table 4. Return Codes for the IRRDBU00 Utility

Hex (Decimal)	Explanation
0 (0)	Successful completion without error.
4 (4)	Error locking or unlocking a data set.
8 (8)	Failed profile. Conversion is incomplete.
10 (16)	Terminating error. Conversion incomplete or not started.
14 (20)	Open of SYSPRINT DCB failed.
20 (32)	RACF is not enabled. Process ends.

Table 5. Return Codes for the IRRIRA00 Utility

Hex (Decimal)	Explanation
0 (0)	Successful completion.
4 (4)	Warning message issued. <ul style="list-style-type: none"> • Database already at requested stage. • Backup database not converted, currently inactive.
C (12)	I/O error reading or writing the ICB.
10 (16)	Terminating error. One of the following occurred: <ul style="list-style-type: none"> • RACF is not active. • Cannot establish recovery. • Parameter error - unsupported stage value. • Parameter error - unrecognized keyword. • Parameter error - not permitted to convert from current stage to stage value specified. • Failure reading/ updating profile. • Conversion cannot be performed because system is in read-only mode. • Failure writing to CF. • Conversion cannot be performed because templates are downlevel.
14 (20)	Unable to open SYSPRINT.
20 (32)	RACF not enabled.

Appendix. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen-readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen-readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using it to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Volume I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

Notices

This information was developed for products and services offered in the USA. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This product contains code licensed from RSA Data Security Incorporated.



Programming interface information

This primarily documents information that is not intended to be used Programming Interface information of the Security Server.

This also documents intended Programming Interfaces that allow the customer to write programs that obtain the services of the Security Server.

This information is identified where it occurs by an introductory statement to a chapter or section.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX/6000
AT
BookManager
C/370
CICS
CICS/ESA
Current
DB2
DFSMS
DFSMSdfp
DFSMS/MVS
DFSORT
e-business
eServer
IBM
IBMLink
IMS
Language Environment
Library Reader
MVS/DFP
MVS/ESA
MVS/XA
OS/2
OS/390
RACF
Redbooks
Resource Link

System/390
S/390
TalkLink
VM/ESA
VM/XA
VTAM
z/OS
z/OS.e
z/VM
zSeries

NetView, Tivoli, Tivoli Management Environment, TME, TME 10, and TME 10 Global Enterprise Manager are trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the United States, other countries, or both.

Lotus and Lotus Notes are trademarks of Lotus Development Corporation in the United States, or other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Index

A

- abend codes 295
- accessibility 313
- ADDGROUP command
 - messages 47
- ADDSD command
 - messages 63
- ADDUSER command
 - messages 49
- administration
 - classroom courses viii
- ALTDSD command
 - messages 102
- ALTGROUP command
 - messages 95
- ALTUSER command
 - messages 98

C

- CACHECLS profile messages
 - messages 248
- classroom courses, RACF viii
- codes
 - abend 295
 - completion 295
 - descriptor codes 1, 131
 - RACF manager return codes 307
 - RACF utility return codes 310
 - routing codes 2, 132
- completion codes 295
- CONNECT command
 - messages 51
- courses about RACF viii

D

- data security monitor (DSMON)
 - messages 119
- DELDSD command
 - messages 63
- DELGROUP command
 - messages 57
- DELUSER command
 - messages 55
- descriptor codes 1, 131
- disability 313
- DISPLAY command
 - messages 220
- documents, licensed ix
- DSMON (data security monitor)
 - messages 119
- dynamic parse
 - messages 148
- dynamic started task operator messages 142

F

- File allocation
 - messages 281

I

- ICH operator messages 1
- ICH000 series of messages 2
- ICH00000 series of messages 47
- ICH01000 series of messages 49
- ICH02000 series of messages 51
- ICH03000 series of messages 53
- ICH04000 series of messages 55
- ICH05000 series of messages 57
- ICH06000 series of messages 58
- ICH08000 series of messages 61
- ICH09000 series of messages 63
- ICH10000 series of messages 69
- ICH11000 series of messages 73
- ICH12000 series of messages 77
- ICH13000 series of messages 79
- ICH14000 series of messages 80
- ICH15000 series of messages 91
- ICH20000 series of messages 95
- ICH21000 series of messages 98
- ICH22000 series of messages 102
- ICH300 series of messages 4
- ICH30000 series of messages 107
- ICH31000 series of messages 108
- ICH32000 series of messages 111
- ICH35000 series of messages 112
- ICH400 series of messages 5
- ICH500 series of messages 24
- ICH51000 series of messages 115
- ICH64000 series of messages 117
- ICH66000 series of messages 119
- ICH700 series of messages 41
- ICH70000 series of messages 124
- ICH800 series of messages 42
- ICH900 series of messages 43
- IKJ messages 293
- initialization messages 24
- Internal reorganization of aliases utility (IRRIRA00)
 - messages 186
- IRR operator messages 131
- IRR000 series of messages 132
- IRR16000 series of messages 148
- IRR400 series of messages 134
- IRR500 series of messages 139
- IRR52000 series of messages 148
- IRR61000 series of messages 168
- IRR62000 series of messages 169
- IRR63000 series of messages 176
- IRR65000 series of messages 182
- IRR66000 series of messages 186
- IRR67000 series of messages 190
- IRR68000 series of messages 200

- IRR71000 series of messages 202
- IRR800 series of messages 139, 140, 142, 143
- IRR8000 series of messages 127
- IRRA0000 series of messages 203
- IRRADU00 utility
 - messages 190
- IRRB0000 series of messages 204
- IRRC0000 series of messages 212
- IRRD0000 series of messages 220
- IRRD100 series of messages 222
- IRRD200 series of messages 230
- IRRDBU00 utility
 - messages 190
 - return codes 311
- IRRDPI00 command
 - messages 139, 148
- IRRE0000 series of messages 233
- IRRF000 series of messages 236
- IRRG000 series of messages 237
- IRRH000 series of messages 239
- IRRI000 series of messages 241
- IRRIRA00 utility
 - return codes 311
- IRRJ000 series of messages 245
- IRRK000 series of messages 246
- IRRL0000 series of messages 247
- IRRL1000 series of messages 248
- IRRM000 series of messages 250
- IRRMIN00 utility
 - messages 127
- IRRN000 series of messages 261
- IRRO000 series of messages 262
- IRRP000 series of messages 263
- IRRQ000 series of messages 267
- IRRR000 series of messages 267
- IRRRID00 utility
 - messages 200
- IRRS000 series of messages 274
- IRRT000 series of messages 276
- IRRU000 series of messages 281
- IRRUT100 utility
 - messages 168
 - return codes 310
- IRRUT200 utility
 - messages 169
 - return codes 310
- IRRUT400 utility
 - messages 182
 - return codes 311
- IRRV000 series of messages 282
- IRRX0000 series of messages 287

K

- keyboard 313

L

- licensed documents ix
- LISTDSD command
 - messages 112

- LISTGRP command
 - messages 111
- LISTUSER command
 - messages 107
- LookAt message retrieval tool ix

M

- message retrieval tool, LookAt ix
- miscellaneous messages 124
- miscellaneous RACF ICH messages 115

P

- PASSWORD command
 - messages 61
- PERMIT command
 - messages 58
- PKI
 - messages 230
- publications
 - on CD-ROM viii
 - softcopy viii

R

- RACDCERT command
 - messages 222
- RACF
 - classroom courses viii
 - messages 147
 - publications
 - on CD-ROM viii
 - softcopy viii
- RACF administration
 - classroom courses viii
- RACF block update command (BLKUPD)
 - messages 176
- RACF commands
 - messages 45
- RACF coupling facility related
 - messages 287
- RACF database
 - initialization messages 127
 - initialization utility messages 127
 - split/merge utility (IRRUT400) and (IRRIRA00)
 - messages 182
 - unload utility messages 190
- RACF initialization messages 24
- RACF manager
 - error messages 115
 - return codes 307
- RACF messages
 - miscellaneous 124
 - miscellaneous ICH 115
- RACF operational modes
 - messages 287
- RACF processing messages 5, 134
- RACF remove ID utility messages 200
- RACF report writer
 - messages 117

- RACF security topics
 - classroom courses viii
- RACF SMF data unload utility messages 190
- RACF status messages 41
- RACF subsystem
 - messages 203
- RACF utilities
 - return codes 310
- RACF/DB2 external security module messages 143
- RACFRW (RACF report writer)
 - messages 117
- RACLINK command
 - messages 246, 274, 276
- RACROUTE REQUEST=AUTH VLF operator
 - messages 139
- RACROUTE REQUEST=LIST
 - messages 247
- RACROUTE REQUEST=VERIFY messages 4
- RACROUTE REQUEST=VERIFY NJE operator
 - messages 140, 143
- RACVAR function for REXX execs
 - messages 202
- RALTER command
 - messages 73
- RDEFINE command
 - messages 69
- RDELETE command
 - messages 77
- REMOVE command
 - messages 53
- REQUEST=AUTH operator messages 42
- REQUEST=DEFINE operator messages 43
- return codes
 - RACF manager 307
 - RACF utility 310
- REXX RACVAR function
 - messages 202
- RLIST command
 - messages 79
- routing codes 2, 132
- RRSF (RACF remote sharing facility)
 - messages 263
- RRSF connection local transaction program
 - messages 245
- RRSF connection receive transaction program
 - messages 261
- RRSF connection send transaction program
 - messages 262
- RRSF connection task
 - messages 267
- RRSF enveloping
 - messages 282
- RRSF handshaking
 - messages 241
- RRSF output handling task
 - messages 267, 276
- RRSF parmlib and initialization
 - messages 237
- RRSF send request handling task
 - messages 236

- RVARY command
 - messages 91

S

- SAF initialization operator messages 2
- SEARCH command
 - messages 108
- security topics for RACF
 - classroom courses viii
- series of messages 143
- SET command
 - messages 239
- SETROPTS command
 - messages 80
- shortcut keys 313
- SIGNOFF command
 - messages 233
- status messages 41
- system operator messages 1, 131
 - dynamic started task (IRR800) 142
 - IRRDPI00 command (IRR500) 139
 - RACF initialization (ICH500) 24
 - RACF processing (ICH400) 5
 - RACF processing (IRR400) 134
 - RACF status (ICH700) 41
 - RACF/DB2 external security module messages 143
 - REQUEST=AUTH (ICH800) 42
 - REQUEST=AUTH VLF (IRR800) 139
 - REQUEST=DEFINE (ICH900) 43
 - REQUEST=VERIFY (ICH300) 4
 - REQUEST=VERIFY NJE (IRR800) 140, 143
 - SAF initialization (ICH000) 2
 - UID/GID mapping (IRR800) 142
 - VERIFY and VERIFYX (IRR000) 132
 - VLF Cache 143

T

- TARGET command
 - messages 250

U

- UID/GID mapping operator messages 142

V

- VERIFY and VERIFYX operator messages 132
- VLF Cache operator messages 143

Readers' Comments — We'd Like to Hear from You

z/OS
Security Server RACF
Messages and Codes

Publication No. SA22-7686-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Complete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to find	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to understand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Well organized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicable to your tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.



Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape



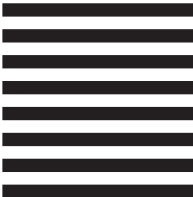
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY
12601-5400



Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line



Program Number: 5694-A01, 5655-G52

Printed in U.S.A.

SA22-7686-03

